

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-045507

(43)Date of publication of application : 16.02.1999

(51)Int.Cl.

G11B 20/10

G06F 12/14

G09C 1/00

H04L 9/08

H04L 9/32

(21)Application number : 09-198638

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 24.07.1997

(72)Inventor : ANDO HIDEO

NAKAGAWA MASAKI

KOJIMA TADASHI

ISHIZAWA YOSHIYUKI

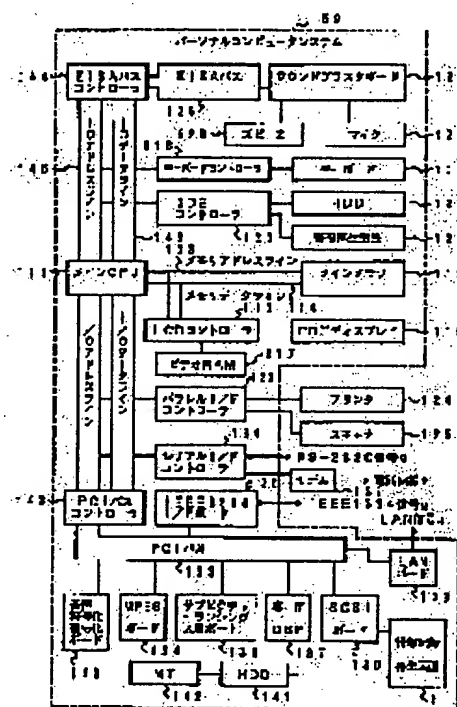
(54) INFORMATION REPRODUCING DEVICE, RECOGNITION DEVICE, AND INFORMATION PROCESSING SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To perform data transmission between a reproducing device and a processing board and to reduce the load on a main control part, by discriminating the kind of reproduced information and setting certification on a specified object to be certified based on the discriminating result.

SOLUTION: At the time of reproducing information, various kinds of streams of information are separated and extracted from a program stream, and are transferred without intervention of a main CPU 111 and directly through a PCI bus 133 to a sound coding and decoding board 136, an MPG board 134 and a board 135 for sub-picture-run-length by an information recording and reproducing device 1. Similarly to the information recording and reproducing device 1, each individual separated and extracted stream is also transferred via an I/O data line 146 and the PCI bus 133 without intervention of the main CPU 111 to the boards 134 and 135 and an SCSI board 136, by the information

reproducing device 122. Thus, without intervention of the main CPU 111, data can be transferred between the information recording and reproducing device and also the information reproducing device 122 and the individual boards 134, 135 and 136 respectively, thus reducing the load on the CPU 111.



LEGAL STATUS

[Date of request for examination]

16.07.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than

the examiner's decision of rejection or
application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-45507

(43) 公開日 平成11年(1999) 2月16日

(51) Int.Cl.⁸

識別記号

F I

G 1 1 B 20/10

G 1 1 B 20/10

D

G 0 6 F 12/14

3 2 0

G 0 6 F 12/14

3 2 0 B

G 0 9 C 1/00

6 6 0

G 0 9 C 1/00

6 6 0 G

H 0 4 L 9/08

H 0 4 L 9/00

6 0 1 A

9/32

6 0 1 E

審査請求 未請求 請求項の数28 O L (全 33 頁) 最終頁に続く

(21) 出願番号

特願平9-198638

(22) 出願日

平成9年(1997) 7月24日

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 安東 秀夫

神奈川県川崎市幸区柳町70番地 株式会社

東芝柳町工場内

(72) 発明者 中河 正樹

神奈川県川崎市幸区柳町70番地 株式会社

東芝柳町工場内

(72) 発明者 小島 正

神奈川県川崎市幸区柳町70番地 株式会社

東芝柳町工場内

(74) 代理人 弁理士 鈴江 武彦 (外6名)

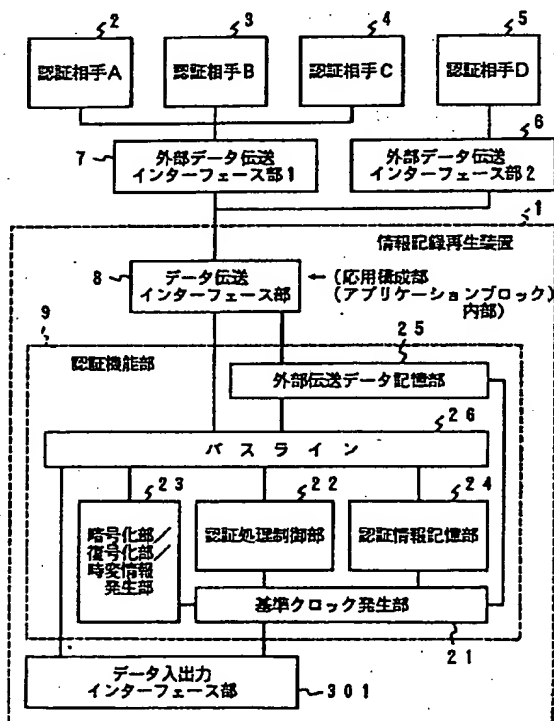
最終頁に続く

(54) 【発明の名称】 情報再生装置、認識装置、情報処理システム

(57) 【要約】

【課題】 この発明は、メインの制御部が介在せずに、情報記録再生装置と各処理ボードとの情報の伝送を行えることができ、メインCPUの負担を軽減でき、情報伝送期間中にメインCPUが他の処理を行うことができる。

【解決手段】 この発明は、情報記録再生装置1が認証機能を持ち、メインCPU111を介さずに直接、MP EGボード134、サブピクチャーランレングス用ボード135、音声符号化復号化ボード136に情報を伝送するようにしたものである。



【特許請求の範囲】

【請求項 1】 情報記録媒体に記録されている情報を再生する情報再生装置において、
上記情報再生装置以外の特定の認証相手に対して認証を行う認証手段と、

を具備したことを特徴とする情報再生装置。

【請求項 2】 上記認証手段が、上記認証相手と独自に相互認証と共通の暗号鍵の伝送を行い、かつ上記認証相手との間で上記共通の暗号鍵を利用した暗号化情報を伝送することを特徴とする請求項 1 に記載の情報再生装置。

【請求項 3】 上記認証手段が、上記共通の暗号鍵を用いて情報を暗号化する暗号化部、あるいは暗号化された情報を復号化する復号化部を有することを特徴とする請求項 2 に記載の情報再生装置。

【請求項 4】 上記共通の暗号鍵が、14 ビット以上のサイズを有することを特徴とする請求項 2 に記載の情報再生装置。

【請求項 5】 上記暗号化部、あるいは上記復号化部が、ランダム信号発生器を有し、このランダム信号発生器からのランダム信号を用いて暗号化あるいは復号化を行うことを特徴とする請求項 3 に記載の情報再生装置。

【請求項 6】 上記認証手段が、暗号鍵を発生する発生手段を有し、上記認証相手に対して少なくとも上記暗号鍵を伝送して共有化することを特徴とする請求項 1 に記載の情報再生装置。

【請求項 7】 上記暗号鍵が、14 ビット以上のサイズを有することを特徴とする請求項 6 に記載の情報再生装置。

【請求項 8】 上記認証手段が、時変情報を発生する発生手段を有し、この発生手段からの時変情報を用いて暗号化あるいは復号化を行うことを特徴とする請求項 3 に記載の情報再生装置。

【請求項 9】 上記発生手段が、ランダム信号発生器で構成されることを特徴とする請求項 8 に記載の情報再生装置。

【請求項 10】 上記認証手段が、第 1 の暗号鍵を発生させる発生手段と、上記認証相手から送られた第 2 の暗号鍵を用いて上記第 1 の暗号鍵を暗号化する暗号化手段と、この暗号化手段により暗号化された上記第 1 の暗号鍵を上記認証相手に伝送する伝送手段とを有することを特徴とする請求項 1 に記載の情報再生装置。

【請求項 11】 上記認証手段が、上記発生手段により発生された第 1 の暗号鍵、上記認証相手から送られた第 2 の暗号鍵の少なくともいずれかを記憶する記憶手段を有することを特徴とする請求項 10 に記載の情報再生装置。

【請求項 12】 情報記録媒体に記録されている情報を再生する情報再生装置において、
上記情報記録媒体から再生した情報の種類を判別する判

別手段と、

この判別手段の判別結果に基づいて複数の認証相手の 1 つを認証相手と設定する設定手段と、

を具備したことを特徴とする情報再生装置。

【請求項 13】 上記情報記録媒体に記録されている情報が、少なくとも複数のパケットの集合体として記録され、上記判別手段が少なくともパケット内に記録して有る情報に基づき認証相手を判別することを特徴とする請求項 12 に記載の情報再生装置。

【請求項 14】 上記設定手段が、複数の認証相手の候補に対し、伝送したい情報の種類を知らせることにより、該当する認証相手を設定することを特徴とする請求項 12 に記載の情報再生装置。

【請求項 15】 上記認証手段が、上記認証相手に伝送する情報を記憶する記憶手段を有することを特徴とする請求項 1 に記載の情報再生装置。

【請求項 16】 上記認証手段が、独自に基準クロックを発生する発生手段を有し、この発生手段からの基準クロックに基づいて認証を行うことを特徴とする請求項 15 に記載の情報再生装置。

【請求項 17】 上記認証手段が、上記認証相手との間で事前に共有化され、上記第 2 の暗号鍵を暗号化あるいは復号化するための第 3 の暗号鍵をあらかじめ記憶する記憶手段を有し、この記憶手段に記憶されている第 3 の暗号鍵を用いて上記第 2 の暗号鍵を暗号化あるいは復号化する手段とを有することを特徴とする請求項 10 に記載の情報再生装置。

【請求項 18】 情報記録媒体に記録されている情報を再生する情報再生装置において、

上記情報再生装置以外の特定の認証相手に対して情報の伝送を行う通信手段と、

この通信手段を用いて上記認証相手に対して認証を行う認証手段と、

を具備したことを特徴とする情報再生装置。

【請求項 19】 上記認証手段が、上記認証相手と独自に相互認証と共通の暗号鍵の伝送を上記通信手段を用いて行い、かつ上記認証相手との間で上記共通の暗号鍵を利用した暗号化情報を上記通信手段を用いて伝送することを特徴とする請求項 1 に記載の情報再生装置。

【請求項 20】 認証処理を行う認証処理制御部と認証処理の内容を記憶する認証情報記憶部とを具備し、
上記認証処理制御部による認証処理の履歴を上記認証情報記憶部に逐次記憶することにより、複数の認証相手との間の並行認識処理を可能とすることを特徴とする認証装置。

【請求項 21】 複数の認証相手から個々に第 1 の暗号鍵を受け取る受け取り手段と、

複数の認証相手に対して個々の第 2 の暗号鍵を発行する発行手段と、

上記認証相手から受け取った第 1 の暗号鍵と認証相手に

対して発行した第2の暗号鍵を用いて個々の認証相手との間で共通の暗号鍵を作成する作成手段と、
複数の認証相手に対して別々に上記各手段に対する処理の履歴を記憶する記憶手段と、
を具備したことを特徴とする認証装置。

【請求項22】 上記発行手段が、時変情報を発生する発生手段を有し、この発生手段により発生される時変情報を用いて複数の認証相手に対して異なる第2の暗号鍵を発行することを特徴とする請求項21に記載の認証装置。

【請求項23】 複数の認証相手から個々に第1の暗号鍵を受け取るステップと、
複数の認証相手に対して個々の第2の暗号鍵を発行するステップと、
上記認証相手から受け取った第1の暗号鍵と認証相手に対して発行した第2の暗号鍵を用いて個々の認証相手との間で共通の暗号鍵を作成するステップとを有し、
複数の認証相手に対して別々に上記各ステップに対する処理の履歴を逐次記憶し、この記憶されている処理の履歴により、複数の認証処理を並行して実行することを特徴とする認証装置。

【請求項24】 少なくとも暗号鍵の発行とこの発行される暗号鍵に基づいた情報の暗号化と上記発行される暗号鍵に基づいた情報の復号化を行う認識装置において、
上記暗号鍵の発行、情報の暗号化、情報の復号化を行う際に用いるランダム信号を発生する発生手段を具備していることを特徴とする認証装置。

【請求項25】 認証相手からの第1の暗号鍵を受け取る受け取り手段と、
認証相手に対する第2の暗号鍵を発行する発行手段と、
上記認証相手から受け取った第1の暗号鍵と認証相手に対して発行した第2の暗号鍵を用いて認証相手との間で共通の第3の暗号鍵を作成する作成手段と、
情報を上記第3の暗号鍵を用いて暗号化する暗号化手段と、
暗号化されている情報を上記第3の暗号鍵を用いて復号化する復号化手段とを具備し、
上記作成手段、暗号化手段、復号化手段が1つの回路で構成されることを特徴とする認証装置。

【請求項26】 情報を再生する情報再生装置と、この情報再生装置により再生される情報を処理する情報処理回路と、上記情報再生装置と上記情報処理回路を制御するメインCPUとからなる情報処理システムにおいて、
上記メインCPUを介在せずに、上記情報再生装置と上記情報処理回路との間で相互認証を行うことを特徴とする情報処理システム。

【請求項27】 第1の装置と複数の第2の装置の間で相互認証を行うことにより情報の伝送を行う情報処理システムにおいて、
上記第1の装置が、

識別用の情報を出力する第1の出力手段と、

この第1の出力手段に回答して上記第2の装置から供給される第1の暗号化キーに基づいて、あらかじめ記憶されている第2の暗号化キーを暗号化する第1の暗号化手段と、

上記識別用の情報に基づいて第3の暗号化キーを作成する第1の作成手段と、

上記第1の暗号化手段により暗号化された第2の暗号化キーと、上記第1の作成手段により作成された第3の暗号化キーとを出力する第2の出力手段と、

この第2の出力手段に回答して上記第2の装置から供給される暗号化されている第4の暗号化キーを上記作成手段により作成された第3の暗号化キーを用いて復号化する第1の復号化手段と、

この第1の復号化手段により復号化された第4の暗号化キーと上記第2の暗号化キーとに基づいて共通鍵を生成する第1の生成手段と、

この第1の生成手段により生成された共通鍵を用いて情報の符号化、復号化を行う第1の処理手段とからなり、
上記第2の装置が、

上記第1の装置から供給される上記識別用の情報に基づいて第1の暗号化キーを作成する第2の作成手段と、

この第2の作成手段により作成された第1の暗号化キーとを出力する第3の出力手段と、

この第3の出力手段に回答して上記第1の装置から供給される第3の暗号化キーに基づいて、あらかじめ記憶されている第4の暗号化キーを暗号化する第2の暗号化手段と、

この第2の暗号化手段により暗号化された第4の暗号化キーを出力する第4の出力手段と、

上記第3の出力手段に回答して上記第1の装置から供給される第2の暗号化キーを上記第2の作成手段により作成された第1の暗号化キーを用いて復号化する第2の復号化手段と、

この第2の復号化手段により復号化された第2の暗号化キーと上記第4の暗号化キーとに基づいて共通鍵を生成する第2の生成手段と、

この第2の生成手段により生成された共通鍵を用いて情報の符号化、復号化を第2の処理手段とからなることを特徴とする情報処理システム。

【請求項28】 第1の装置と複数の第2の装置の間で相互認証を行うことにより情報の伝送を行う情報処理システムにおいて、
上記第1の装置が、

AGID、設定エリア情報、ストリームIDからなる識別用の情報を出力する第1の出力手段と、
時変情報に基づいて第1の暗号化キーを生成する第1の生成手段と、

上記第1の出力手段に回答して上記第2の装置から供給される暗号化されている第1のチャレンジキーを上記識

別用の情報からなる合成キーに基づいて復号化する第1の復号化手段と、

この第1の復号化手段により復号化された第1のチャレンジキーに基づいて、上記第1の生成手段により生成される第1の暗号化キーを暗号化する第1の暗号化手段と、

時変情報に基づいて第2のチャレンジキーを生成する第2の生成手段と、

上記識別用の情報からなる合成キーに基づいて、上記第2の生成手段により生成される第2のチャレンジキーを暗号化する第2の暗号化手段と、

上記第1の暗号化手段により暗号化された第1の暗号化キーと、上記第2の暗号化手段により暗号化された第2のチャレンジキーとを出力する第2の出力手段と、

この第2の出力手段に回答して上記第2の装置から供給される暗号化されている第2の暗号化キーを上記第2の生成手段により生成された第2のチャレンジキーを用いて復号化する第2の復号化手段と、

この第2の復号化手段により復号化された第2の暗号化キーと上記第1の生成手段により生成される第1の暗号化キーとに基づいて共通鍵を生成する第3の生成手段と、

この第3の生成手段により生成された共通鍵を用いて情報の符号化、復号化を行う第1の処理手段とからなり、上記第2の装置が、

上記第1の装置から供給される上記識別用の情報に基づいて第1のチャレンジキーを生成する第4の生成手段と、

この第4の生成手段により生成された第1のチャレンジキーとを出力する第3の出力手段と、

この第3の出力手段に回答して上記第1の装置から供給される暗号化されている第2のチャレンジキーを、上記第1の装置から供給される上記識別用の情報からなる合成キーに基づいて、復号化する第3の復号化手段と、時変情報に基づいて第2の暗号化キーを生成する第5の生成手段と、

上記第3の復号化手段により復号化された第2のチャレンジキーに基づいて、上記第5の生成手段により生成される第2の暗号化キーを暗号化する第3の暗号化手段と、

この第3の暗号化手段により暗号化された第2の暗号化キーを出力する第4の出力手段と、

上記第3の出力手段に回答して上記第1の装置から供給される暗号化されている第1の暗号化キーを上記第4の生成手段により生成された第1のチャレンジキーを用いて復号化する第4の復号化手段と、

この第4の復号化手段により復号化された第1の暗号化キーと上記第5の生成手段により生成される第2の暗号化キーとに基づいて共通鍵を生成する第6の生成手段と、

この第6の生成手段により生成された共通鍵を用いて情報の符号化、復号化を行う第2の処理手段とからなることを特徴とする情報処理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、情報記録媒体に記録されている情報を再生する情報再生装置、認証処理を行う認証装置、第1の装置と複数の第2の装置の間で相互認証を行うことにより情報の伝送を行う情報処理システムに関する。

【0002】

【従来の技術】従来、DVD等の光ディスクに記録されている映像情報、音声情報、静止画情報など混在する情報を光ディスク装置により再生するものが実用化されている。このような光ディスク装置により再生された情報はその情報の種類に応じて異なった処理回路により処理されるようになっている。

【0003】たとえば、情報としてMPEGビデオデータ、オーディオデータ(PCM、AC3)、サブピクチャーデータ、ナビゲーションデータ等からなる場合に、それぞれのデータに合わせた処理ボードにより処理が行われるようになっている。

【0004】この場合、メインの制御部が、一旦それらのデータを取り込み、この取り込んだデータに応じて各処理ボードにデータを配送していた。

【0005】この場合、そのデータ配送の期間中、メインの制御部が占有されてしまうので、光ディスク装置から再生する情報量が多くなるとメインの制御部の負担が増え、長時間メインの制御部が他の処理を行うことができなくなるといった問題がある。

【0006】また、従来、暗号化技術として知られている双方向本人認証方法はRSA(公開鍵暗号のアルゴリズム)のような公開鍵(アシンメトリックキー)を用いた電子署名を用いた方法が良く知られている。

【0007】たとえば、その方法は

1) “チャレンジ”としてAがBにランダムな文字を送信する。

【0008】2) “レポート”としてBはその文字をBが持っている公開鍵でサインしてAへ返送する。AはBが持っている公開鍵を保管している第3者である認証局(CAセンタ)に問い合わせてBから返送された情報を復号化(解読)する。解読結果がAが最初に送信した文字と一致すればBが本人と認める。

【0009】3) “チャレンジ”としてBがAにランダムな文字を送信する。

【0010】4) “レポート”としてAはその文字をAが持っている公開鍵でサインしてBへ返送する。BはAが持っている公開鍵を保管している第3者である認証局(CAセンタ)に問い合わせてBから返送された情報を復号化(解読)する。解読結果がBが最初に送信した文

字と一致すればAが本人と認める。

【0011】が知られている。

【0012】しかしこの方法では公開鍵を保管している第三者（認証局（CAセンタ））を必要とし、しかも双方本人認証毎に通信で公開鍵を保管している第三者である認証局（CAセンタ）に問い合わせる必要があり、処理が非常に煩雑となるという問題がある。

【0013】さらに、第三者が管理する公開鍵を使用する場合には公開鍵が盗まれやすく、セキュリティ保護が難しかった。

【0014】また、相互に暗号鍵を交換し合う方法は従来知られていたが、伝送すべき情報をその暗号鍵で暗号化する以外は、相互に交換し合った暗号鍵の使い方については余り知られて無い。

【0015】さらに、上記の方法では、認証すべき相手の居場所が事前に分かっており、ある送信したい情報が決まってい、送信すべき相手を探したい場合には上記の方法は意味をなさない。このように従来は認証したい相手を探す方法に付いて有効な方法が無かった。

【0016】

【発明が解決しようとする課題】この発明は、メインの制御部が介在せずに、情報再生装置と各処理ボードとのデータの伝送を行えることができ、メインの制御部の負担を軽減でき、情報伝送期間中にメインの制御部が他の処理を行うことができる。

【0017】また、この発明は、非常に簡単な構成で暗号化／復号化（解読）を行える。

【0018】また、この発明は、公開鍵を管理する第三者を置くことなく容易に相互認証可能、つまり第三者の介在や第三者への問い合わせ作業を不要とし、相互認証作業を非常に簡便にしかも信頼性高く行える。

【0019】また、この発明は、伝送し合った暗号鍵で他方の暗号鍵を更に暗号化することにより、公開鍵方式を用いるよりも遙かに暗号化の信頼性が高く、情報漏洩を防げる。

【0020】また、この発明は、情報記録媒体からの情報に付与されている情報の種類を示す情報（ストリームID）から認証相手を同定することにより、各認証相手に対して認証後、各認証相手にパラレルに情報を配信（送信）でき、この結果、各認証相手の負担が相対的に軽減すると共に情報記録媒体から情報再生を開始してから短時間で画面上に表示でき、タイムラグを最小に抑えることができる。

【0021】また、この発明によれば、送信したい情報から認証相手を探すことができ、認証候補相手に対して情報を提供し、該当相手から回答してもらい、その回答結果に基づき相互認証作業に入るという方式により、比較的簡単な方法で認証相手を探すことができる。

【0022】

【課題を解決するための手段】この発明の情報再生装置

は、情報記録媒体に記録されている情報を再生するものにおいて、上記情報再生装置以外の特定の認証相手に対して認証を行う認証手段からなる。

【0023】この発明の情報再生装置は、情報記録媒体に記録されている情報を再生するものにおいて、上記情報記録媒体から再生した情報の種類を判別する判別手段、およびこの判別手段の判別結果に基づいて複数の認証相手の1つを認証相手と設定する設定手段からなる。

【0024】この発明の情報再生装置は、情報記録媒体に記録されている情報を再生するものにおいて、上記情報再生装置以外の特定の認証相手に対して情報の伝送を行う通信手段、およびこの通信手段を用いて上記認証相手に対して認証を行う認証手段からなる。

【0025】この発明の認証装置は、認証処理を行う認証処理制御部と認証処理の内容を記憶する認証情報記憶部とを具備し、上記認証処理制御部による認証処理の履歴を上記認証情報記憶部に逐次記憶することにより、複数の認証相手との間の並行認識処理を可能とする。

【0026】この発明の認証装置は、複数の認証相手から個々に第1の暗号鍵を受け取る受け取り手段、複数の認証相手に対して個々の第2の暗号鍵を発行する発行手段、上記認証相手から受け取った第1の暗号鍵と認証相手に対して発行した第2の暗号鍵を用いて個々の認証相手との間で共通の暗号鍵を作成する作成手段、および複数の認証相手に対して別々に上記各手段に対する処理の履歴を記憶する記憶手段からなる。

【0027】この発明の認証装置は、複数の認証相手から個々に第1の暗号鍵を受け取るステップと、複数の認証相手に対して個々の第2の暗号鍵を発行するステップと、上記認証相手から受け取った第1の暗号鍵と認証相手に対して発行した第2の暗号鍵を用いて個々の認証相手との間で共通の暗号鍵を作成するステップとを有し、複数の認証相手に対して別々に上記各ステップに対する処理の履歴を逐次記憶し、この記憶されている処理の履歴により、複数の認証処理を並行して実行するものである。

【0028】この発明の認証装置は、少なくとも暗号鍵の発行とこの発行される暗号鍵に基づいた情報の暗号化と上記発行される暗号鍵に基づいた情報の復号化を行うものにおいて、上記暗号鍵の発行、情報の暗号化、情報の復号化を行う際に用いるランダム信号を発生する発生手段からなる。

【0029】この発明の認証装置は、認証相手からの第1の暗号鍵を受け取る受け取り手段、認証相手に対する第2の暗号鍵を発行する発行手段、上記認証相手から受け取った第1の暗号鍵と認証相手に対して発行した第2の暗号鍵を用いて認証相手との間で共通の第3の暗号鍵を作成する作成手段、情報を上記第3の暗号鍵を用いて暗号化する暗号化手段、および暗号化されている情報を上記第3の暗号鍵を用いて復号化する復号化手段からなる。

り、上記作成手段、暗号化手段、復号化手段が1つの回路で構成される。

【0030】この発明の情報処理システムは、情報を再生する情報再生装置と、この情報再生装置により再生される情報を処理する情報処理回路と、上記情報再生装置と上記情報処理回路を制御するメインCPUとからなるものにおいて、上記メインCPUを介在せずに、上記情報再生装置と上記情報処理回路との間で相互認証を行う。

【0031】この発明の情報処理システムは、第1の装置と複数の第2の装置の間で相互認証を行うことにより情報の伝送を行うものにおいて、上記第1の装置が、識別用の情報を出力する第1の出力手段と、この第1の出力手段にตอบสนองして上記第2の装置から供給される第1の暗号化キーに基づいて、あらかじめ記憶されている第2の暗号化キーを暗号化する第1の暗号化手段と、上記識別用の情報に基づいて第3の暗号化キーを作成する第1の作成手段と、上記第1の暗号化手段により暗号化された第2の暗号化キーと、上記第1の作成手段により作成された第3の暗号化キーとを出力する第2の出力手段と、この第2の出力手段にตอบสนองして上記第2の装置から供給される暗号化されている第4の暗号化キーを上記作成手段により作成された第3の暗号化キーを用いて復号化する第1の復号化手段と、この第1の復号化手段により復号化された第4の暗号化キーと上記第2の暗号化キーとに基づいて共通鍵を生成する第1の生成手段と、この第1の生成手段により生成された共通鍵を用いて情報の符号化、復号化を行う第1の処理手段とからなり、上記第2の装置が、上記第1の装置から供給される上記識別用の情報に基づいて第1の暗号化キーを作成する第2の作成手段と、この第2の作成手段により作成された第1の暗号化キーとを出力する第3の出力手段と、この第3の出力手段にตอบสนองして上記第1の装置から供給される第3の暗号化キーに基づいて、あらかじめ記憶されている第4の暗号化キーを暗号化する第2の暗号化手段と、この第2の暗号化手段により暗号化された第4の暗号化キーを出力する第4の出力手段と、上記第3の出力手段にตอบสนองして上記第1の装置から供給される第2の暗号化キーを上記第2の作成手段により作成された第1の暗号化キーを用いて復号化する第2の復号化手段と、この第2の復号化手段により復号化された第2の暗号化キーと上記第4の暗号化キーとに基づいて共通鍵を生成する第2の生成手段と、この第2の生成手段により生成された共通鍵を用いて情報の符号化、復号化を第2の処理手段とからなる。

【0032】この発明の情報処理システムは、第1の装置と複数の第2の装置の間で相互認証を行うことにより情報の伝送を行うものにおいて、上記第1の装置が、AGID、設定エリア情報、ストリームIDからなる識別用の情報を出力する第1の出力手段と、時変情報に基づ

いて第1の暗号化キーを生成する第1の生成手段と、上記第1の出力手段にตอบสนองして上記第2の装置から供給される暗号化されている第1のチャレンジキーを上記識別用の情報からなる合成キーに基づいて復号化する第1の復号化手段と、この第1の復号化手段により復号化された第1のチャレンジキーに基づいて、上記第1の生成手段により生成される第1の暗号化キーを暗号化する第1の暗号化手段と、時変情報に基づいて第2のチャレンジキーを生成する第2の生成手段と、上記識別用の情報からなる合成キーに基づいて、上記第2の生成手段により生成される第2のチャレンジキーを暗号化する第2の暗号化手段と、上記第1の暗号化手段により暗号化された第1の暗号化キーと、上記第2の暗号化手段により暗号化された第2のチャレンジキーとを出力する第2の出力手段と、この第2の出力手段にตอบสนองして上記第2の装置から供給される暗号化されている第2の暗号化キーを上記第2の生成手段により生成された第2のチャレンジキーを用いて復号化する第2の復号化手段と、この第2の復号化手段により復号化された第2の暗号化キーと上記第1の生成手段により生成される第1の暗号化キーとに基づいて共通鍵を生成する第3の生成手段と、この第3の生成手段により生成された共通鍵を用いて情報の符号化、復号化を行う第1の処理手段とからなり、上記第2の装置が、上記第1の装置から供給される上記識別用の情報に基づいて第1のチャレンジキーを生成する第4の生成手段と、この第4の生成手段により生成された第1のチャレンジキーとを出力する第3の出力手段と、この第3の出力手段にตอบสนองして上記第1の装置から供給される暗号化されている第2のチャレンジキーを、上記第1の装置から供給される上記識別用の情報からなる合成キーに基づいて、復号化する第3の復号化手段と、時変情報に基づいて第2の暗号化キーを生成する第5の生成手段と、上記第3の復号化手段により復号化された第2のチャレンジキーに基づいて、上記第5の生成手段により生成される第2の暗号化キーを暗号化する第3の暗号化手段と、この第3の暗号化手段により暗号化された第2の暗号化キーを出力する第4の出力手段と、上記第3の出力手段にตอบสนองして上記第1の装置から供給される暗号化されている第1の暗号化キーを上記第4の生成手段により生成された第1のチャレンジキーを用いて復号化する第4の復号化手段と、この第4の復号化手段により復号化された第1の暗号化キーと上記第5の生成手段により生成される第2の暗号化キーとに基づいて共通鍵を生成する第6の生成手段と、この第6の生成手段により生成された共通鍵を用いて情報の符号化、復号化を行う第2の処理手段とからなる。

【0033】

【発明の実施の形態】以下、図面を参照してこの発明の実施の形態に係る情報記録再生装置を説明する。

【0034】図1に認証機能を有する情報記録再生装置

の構成説明図を示す。

【0035】すなわち、情報記録再生装置1は情報記録媒体（光ディスク）201から情報を再生もしくは情報の記録を行う情報記録再生部（物理系ブロック）200、認証機能部9、通信機能部301、コンピュータ接続インターフェース部302、情報記録再生装置1内全体の制御を行う制御部303、および各部を接続するバスライン26から構成されている。

【0036】情報記録再生装置1は通信機能部301を有することによりネットワークを介して独自に情報を伝送できる。特にネットワークサーバの記録装置として使うため、各種の通信機能を持っている。一般にはLAN接続I/F部304を経由して各クライアントに情報の伝送を行う。それに限らず電話回線を使い、LANに直接接続していないクライアントや携帯端末との間の情報伝送も可能になっている。電話回線で伝送する場合、電話番号を指定するためのNCU部305とNCU部306を持つ。アナログ信号で伝送を希望するクライアントまたは携帯端末に対してはモデムI/F部307を介して情報の伝送を行い、デジタル信号での伝送を希望するクライアントまたは携帯端末に対してはISDN I/F部308から情報の伝送を行う。更にPHS機能を内蔵した情報携帯端末との間の情報交換はPHS I/F部309を利用する。

【0037】図2～図6を用いて情報記録再生装置1内にある認証機能部9の内部構造説明と機能説明を行う。

【0038】[1] 認証機能の概要説明（認証機能とは何か）

[1-1] 情報記録再生装置と外部接続相手との間の関係

図2に認証機能部の内部構造とそれに接続される周辺機器との関係を示す。

【0039】上記情報記録媒体201から再生された情報もしくは情報記録媒体201へ記録される情報は情報記録再生装置1内のデータ伝送インターフェース部8を介して外部接続相手との間で伝送される。

【0040】情報伝送相手となる外部接続相手は複数存在し、例えば図2のように認証相手A：2、認証相手B：3、認証相手C：4、認証相手D：5などが接続されている。

【0041】外部接続相手との間の情報伝送を行った場合、例えば外部データ伝送インターフェース部2：6を経て認証相手D：5に接続されたり、外部データ伝送インターフェース部1：7が各認証相手A：2、B：3、C：4へ情報を配送する。

【0042】[1-2] 複数の外部接続相手との間の情報伝送方法

図2のように情報記録再生装置1が複数の接続相手とながり、

1) 情報記録媒体201に記録するあるいは情報記録媒

体201から再生する情報の内容に応じて特定の外部接続相手のみとの情報伝送を行う

2) 複数の異なる内容の情報に応じて同時に複数の外部接続相手とそれぞれ独自に情報伝送を行う

3) 特定の外部接続相手との間で伝送した情報は他の外部接続相手が傍受不可能と言う操作を実行するため

◎外部接続相手との間で情報を暗号化して伝送する

◎暗号化した情報伝送に先立ち、各外部接続相手毎に暗号化用の鍵を共有するを行っている。

【0043】[1-3] 複数の外部接続相手との事前の認証作業

外部接続相手との間で暗号化した情報を伝送する前に、事前の認証作業を行う。

【0044】1) 情報記録媒体201に記録するあるいは情報記録媒体201から再生する情報の内容に応じて適合した外部接続相手（認証相手）を捜す

2) 捜し当てた認証相手（外部接続相手）毎にID番号を発行する

3) 捜し当てた認証相手（外部接続相手）が本物であるかを“チャレンジレスポンス”と言う方法（詳細は後述）を用いて確認する

4) 特定の認証相手のみと共有できる秘密の暗号解読鍵を作成すると言う一連の処理により認証作業が行われる。

【0045】[1-4] ネットワークシステムにおける情報伝送の具体例

上記の概要説明に付いての具体的実施例に従った説明を以下に行う。

【0046】図2に示した接続をネットワークシステムに適応した場合には、情報記録再生装置1はネットワークサーバのメインメモリドライブとして使われる。ネットワークサーバの分散処理に従って情報記録再生装置1が独自に情報の配送・収集を行う。

【0047】ネットワークサーバから情報の配送・収集先のクライアント（のIPアドレスや電話番号）と配送・収集する情報内容を通知された後は、ネットワークサーバのメインCPUを介さずに情報記録再生装置1が直接クライアントと交信を開始する。

【0048】従ってネットワークシステムに適応した場合は認証相手A：2、認証相手B：3、認証相手C：4、認証相手D：5は個々のクライアントマシン（PCなど）を意味する。またデータ伝送インターフェース部8は“LAN用I/F部”もしくは“モデム”や“PHSなどのデジタル通信用I/F部”に対応し、外部データ伝送インターフェース部1：7はネットワーク上の“ファイアーウォール”あるいは“ルーター”“ゲートウェイ”“ブリッジ”などに対応する。1台のクライアントマシン（認証相手D5）につながる外部データ伝送インターフェース部2：6をクライアントマシン内に内蔵されている“LAN用I/F部”もしくは“モデム”

や“PHSなどのデジタル通信用I/F部”に対応するとの解釈もできる。

【0049】上記データ伝送インターフェース部8は、図1に示す通信機能部301内のLAN接続I/F部304、モデムI/F部307、ISDN I/F部308、PHS I/F部309に対応する。

【0050】[1-5] PCシステム内での情報伝送の具体例

PC（パーソナルコンピュータ）システム内での外部接続相手（認証相手）としては以下の2種類の場合が有る

【1-5-1】PC内の記録装置

外部接続相手（認証相手）としてはATAPI（ATAタッチメントパケットインターフェース）やSCSI（スカジー）、IEEE1394（米国電機電子技術者協会企画のシリアルインターフェース）などで接続される“HDD”“CD-ROM”“MO”“PD（相変化型記録ドライブ）”“DVD-ROM”“DVD-RAM”“半導体メモリ”などの記録装置を意味し、データ伝送インターフェース部8、外部データ伝送インターフェース部7、外部データ伝送インターフェース部6はATAPIやSCSI、IEEE1394などのインターフェース部を示す。

【0051】[1-5-2] PC内の信号処理部

外部接続相手（認証相手）としては“MPEGエンコード/デコード部”“サウンドプラスタ部”“オーディオ信号圧縮伸長部”“サブピクチャーランレングス用ボード”“プログラム実行用CPU”などの信号処理部を意味し、データ伝送インターフェース部8、外部データ伝送インターフェース部7、外部データ伝送インターフェース部6はATAPIやSCSI、IEEE1394などのインターフェース部を示す。

【0052】上記情報記録再生装置1としては、たとえば図2に示すデータ伝送インターフェース部8、認証機能部9、データ入出力インターフェース部30を有する後述する情報記録再生部（物理ブロック）200（図9参照）により構成されている。

【0053】上記認証相手も上記認証機能部9と同じ構成のものを有している。認証相手が単体の場合には、後述する認証情報記憶部24の縦1列の情報が記憶される。

【0054】[2] 情報記録媒体201の記録内容と認証相手設定との関係

【2-1】DVD-ビデオにおけるフォーマット構造
DVD-ビデオの情報は大きくVMG（ビデオ マネージャー）とVTS（ビデオ タイトル セット）に分けられる。

【0055】VMG（ビデオ マネージャー）はメニューあるいはタイトルを再生するための制御情報を含み、VTS（ビデオ タイトル セット）は映像データを構成する各種エレメントの構成が同じであるタイトルの集

まりになっている。

【0056】VTS（ビデオ タイトル セット）内の再生用の映像データの集まりをVOBS（ビデオ オブジェクト セット）と呼ぶ。VOBSはMPEG2のPS（プログラムストリーム）構造を取るVOB（ビデオ オブジェクト）の集まりである。

【0057】また各VOBは、制作者の目的に応じたシーン単位にセル（セル）に分割する事が可能である。

【0058】さらに各セルは複数のVOBU（ビデオ オブジェクト ユニット）から構成されている。

【0059】[2-2] DVD-ビデオにおける情報記録媒体201の記録内容

VOBU内部は“ビデオ情報”“オーディオ情報”“サブピクチャー情報”“ナビゲーション情報”が混在して記録され、それぞれの情報が『バック』と呼ばれるブロック毎のかたまり単位で時分割されて情報記録媒体201に記録されている。

【0060】図3に情報記録媒体201に記録されているVOBU内部構造説明図を示す。ディスク形状の情報記録媒体201では内周から外周に向かってスパイラル状にトラックが連続しており、図3はそのトラックに沿って記録して有る情報の一部を示している。

【0061】例えば図3の“aバック10a”がビデオ情報が記録されている“ビデオバック”に対応し、“bバック10b”がオーディオ情報が記録されている“オーディオバック”に対応する。オーディオバックはAC-3またはPCM形式でオーディオ情報が記録されている。さらに一例として“cバック10c”が字幕や挿入静止画などの情報を持つ“サブピクチャーバック”、“dバック10d”が次のアクセス先などを示す“ナビゲーションバック”に対応する。

【0062】各バックの集合により形成されるストリームとしては、ビデオデータストリーム、オーディオデータストリーム、サブピクチャーデータストリーム、ナビゲーションデータストリーム、ドルビー/リニアオーディオデータストリーム等からなる。

【0063】[2-3] DVD-ビデオにおける記録内容と認証相手設定との関係

図2に示した情報記録再生装置1がPC（パーソナルコンピュータ）に接続されている場合には“[1-5-2] PC内の信号処理部”で説明したように各認証相手はPC内に組み込まれている各種信号処理用ボードに対応する。例えば認証相手A：2がMPEGエンコーダ/デコーダボードを意味し、認証相手B：3がAC-3またはPCMのデコードボード、あるいはサウンドプラスタボードやMPEGオーディオのエンコーダ/デコーダボードに対応する。更に例として認証相手C：4がサブピクチャーランレングス用ボードやキャラクタージェネレーターボードに対応し、認証相手D：5がSCSIラインなどを經由してPCIバス、メインCPUのI/O

データラインを経て到達するPCのメインCPUに対応させる事ができる。

【0064】上記情報記録再生装置1に内蔵される認証機能部9では図3に示される情報記録媒体201上の記録情報の内、aパック10aのみの情報を切り出して取り出し、認証相手A:2に伝送する。同様に認証機能部9ではbパック10b部分を抜き出して認証相手B:3へ伝送し、cパック10c部分を抜き出して認証相手C:4へ伝送する。

【0065】また例えばナビゲーションパックの情報であるdパック10d情報を認証相手D:5であるPCのメインCPUが受け取り、その情報に応じて次にアクセスする位置を判断する。

【0066】[2-4] DVD-ビデオにおける情報内容の識別方法

図3に示した各パック内部は、図4に示すようにパックヘッダ11とパケット12に分かれている。

【0067】パックヘッダ11は4バイトのパックスタートコード、6バイトのシステムクロックリファレンス、3バイトの転送レート表示コードなどから構成されている。

【0068】パケット12は更にパケットヘッダ13と伝送される情報内容14に分かれる。パケットヘッダ13内には3バイトのパケットスタートコードや1バイトのストリームIDが含まれている。

【0069】このパケットヘッダ13内のストリームIDに伝送される情報の種類(ストリーム)が記述されている。具体的には

○ストリームIDが“11100000”の時には伝送される情報内容14がビデオ情報(ビデオストリーム)を意味し、そのパケット12を含むパックはビデオパックを構成する。

【0070】○ストリームIDが“110X0***” (***)はデコーディングオーディオストリーム番号)の時には伝送される情報内容14がMPEGオーディオに基づくオーディオ情報(オーディオストリーム)を意味し、そのパケット12を含むパックはオーディオを構成する。

【0071】○ストリームIDが“10111101”の時には伝送される情報内容14がプライベートストリーム1である事を意味し、“MPEGオーディオ以外のオーディオ情報”か“サブピクチャー情報”がそれに含まれる。

【0072】○ストリームIDが“10111111”の時には伝送される情報内容14がナビゲーション情報(プライベートストリーム2)を意味し、そのパケット12を含むパックはナビゲーションパックを構成する。

【0073】となっている。特にストリームIDが“10111101”のプライベートストリーム1の場合には、図4の“伝送される情報内容14”の最初に、詳細

な情報の種類を示すサブストリームID(1バイト)が記録されている。具体的には

○サブストリームIDが“001*****” (***)はデコーディングサブピクチャー番号)の時には伝送される情報内容14がサブピクチャー 情報(サブピクチャーストリーム)を意味し、そのパケット12を含むパックはサブストリームパックを構成する。

【0074】○サブストリームIDが“10000***” (***)はデコーディングオーディオストリーム番号)の時には伝送される情報内容14が Dolby AC-3を意味し、そのパケット12を含むパックはオーディオパックを構成する。

【0075】○サブストリームIDが“10100***” (***)はデコーディングオーディオストリーム番号)の時には伝送される情報内容14がリニアPCMを意味し、そのパケット12を含むパックはオーディオパックを構成する。

【0076】となっている。

【0077】このように情報記録媒体201から再生される情報に対して、図2の認証機能部9で図4のパケット12内に記録されているストリームIDとサブストリームIDを読み取り、各パック10a~10dの情報の種類を識別する。

【0078】[2-5] プログラムソフトにおける記録内容と認証相手設定との関係

DVD-ビデオではビデオ情報やオーディオ情報というコンテンツ情報のみが記録されているが、コンピュータシステム上では更にテキスト情報やアプリケーション実行用のソフトプログラムが混在している。PCの分散処理に対応して情報記録再生装置1がPCのCRTに表示されている画面を受信したり、同時にHDDやCD-ROMなどの記録装置からソフトプログラムや音声/ビデオ情報を受信する必要が生じる。

【0079】特に音声情報やビデオ情報を伝送する場合には途中で途切れないようにする工夫が必要となる。そのためビデオ情報と音声情報やソフトプログラム、テキスト情報を同時に転送する場合にはビデオ情報を細かくブロック毎に区切り、その合間に他の情報を断続的に入れ込む必要がある。従って情報記録再生装置1が外部から各種の情報を受信し、情報記録媒体201に記録するにはデータ伝送インターフェース部8に入力される情報は図3のように情報種類毎にパック構造またはパケット構造を持ってブロック化され、時分割されている。

【0080】PCシステムの場合は受信した情報をファイル形式で情報記録媒体201に記録する。各ファイル名には拡張子が付けられ、“TXT” “WAV” “BMP” “JPEG” “MPEG” など拡張子(ストリームIDの代りになる)により情報種類を識別できる。

【0081】[2-6] ネットワークシステムにおける記録内容と認証相手設定との関係

ネットワークシステムの場合には伝送情報毎の送信／受信先クライアントマシンのIPアドレスやモデムを用いる場合の電話番号をサーバ本体のメインCPUから指示を受ける。図3のように複数情報を時分割して伝送する以外に同一の情報を一度にまとめて伝送する場合もある。

【0082】【3】認証機能部9内部構造の簡易説明と情報伝送方法

【3-1】認証機能部9内の構成要件

認証機能部9内部の概略構造を図2に示す。認証機能部9は“基準クロック発生部21”“認証処理制御部22”“暗号化部／復号化部／時変情報発生部23”“認証情報記憶部24”“外部伝送データ記憶部25”と各部間の情報の入出力を媒介する共通の“バスライン26”から構成される。

【0083】【3-2】認証処理制御部22

認証処理制御部22では

◎パケット12内のストリームID、サブストリームIDを読み取り、対応する認証相手2～5の割り出し処理

◎認証相手2～5毎のID番号の発行処理

◎認証相手2～5との事前の認証作業と認証相手2～5毎の独自の共通暗号鍵（バスキー）の作成処理

◎作成した暗号鍵を用いた情報の暗号化処理

◎作成した暗号鍵を用いた暗号化された情報の復号化処理と言ういっさいの認証関連処理の実行制御を行う。

【0084】【3-3】認証情報記憶部24

認証情報記憶部24は半導体メモリ素子（たとえばEEPROM）で構成され、認証関連処理に必要な

◎暗号鍵作成のための必要情報

◎認証相手毎に作成した暗号鍵情報

◎認証相手毎に行う後述する一連の認証手順履歴情報が記録される。

【0085】【3-4】暗号化部／復号化部／時変情報発生部23

暗号化部／復号化部／時変情報発生部23では認証関連処理に必要な

“◎暗号鍵の作成” “◎暗号化” “◎復号化”の実行を行う。

【0086】【3-5】外部伝送データ記憶部25

各認証相手2～5の間では暗号化された情報の送受信が行われる。この送受信時に使われる暗号化された情報を外部伝送データ記憶部25に記録している。

【0087】上記情報記録再生装置1内のデータ入出力インターフェース部30から出力された情報記録媒体201からの再生情報はバスライン26を経由して暗号化部／復号化部／時変情報発生部23に入り、そこで暗号化された後、再びバスライン26を経由して外部伝送データ記憶部25に保存される。暗号化された情報を外部に伝送する場合はデータ伝送インターフェース部8が直接この外部伝送データ記憶部25からデータを読み出

す。（情報記録媒体201からのデータ再生時）

各認証相手2～5から受信した暗号化された情報も、データ伝送インターフェース部8から直接この外部伝送データ記憶部25に一時的に保存される。この情報を情報記録媒体201に記録する場合には暗号化された情報が外部伝送データ記憶部25からバスライン26を経由して暗号化部／復号化部／時変情報発生部23に入る。暗号化部／復号化部／時変情報発生部23で復号化された後、バスライン26を経由して情報記録再生部（物理系ブロック）200内のデータ入出力インターフェース部30へ送られる。（情報記録媒体201へのデータ記録時）

【3-6】基準クロック発生部21

認証機能部9内では独自のクロックを持って認証関連処理を行っている。この独自のクロックを基準クロック発生部21で作っている。

【0088】この基準クロック発生部21で作られた基準クロックはデータ入出力インターフェース部30へ送られ、この基準クロックに従ってECCエラー訂正された再生情報が後述する情報記録再生部200から取り出される。更にこの基準クロックに従って暗号化処理が施され、この基準クロックのタイミングで暗号化された情報が外部伝送データ記憶部25に記憶される。

【0089】データ伝送インターフェース部8で処理実行されるタイミングはこの基準クロック発生部21で作られた基準クロックのタイミングとは異なり、外部データ伝送インターフェース部1／2：7／6との間で取り交わされる通信プロトコルのタイミングに沿って処理実行される。またデータ伝送インターフェース部8ではこの通信プロトコルのタイミングに従って外部伝送データ記憶部25に記憶して有る暗号化情報を取り出し、外部へ転送する。

【0090】外部伝送データ記憶部25はバッファとして作用しオーディオデータ等の間欠もキープできる。

【0091】【3-7】通信用プロトコル変換とタイミング確保

“【2-5】プログラムソフトにおける記録内容と認証相手設定との関係”で記述したように音声情報やビデオ情報を含む混在情報を同時に伝送する場合には、音声情報やビデオ情報が途中で途切れないように一定周期で特定量以上の音声情報やビデオ情報を時分割伝送する必要がある。このようにデータ伝送インターフェース部8でプロトコル変換を行う時にデータ構造の組み替えを行っている。

【0092】“【2-1】DVD-ビデオにおけるフォーマット構造”で説明したようにDVD-ビデオではMPEG2のPS（プログラム ストリーム）構造に従って情報記録媒体201上に情報が記録されている。しかし“【1-4】ネットワークシステムにおける情報伝送の具体例”や“【1-5-1】PC内の記録装置”に示

したような利用方法の場合には外部データ伝送インターフェース部1/2:7/6との間で送受信する情報のフォーマット構造はTS(トランスポート ストリーム)が望ましい。TSは188バイト固定長の比較的短いパケット単位を使用し、PSとはパケットサイズ、パケット構造が異なる。(藤原洋:最新MPEG教科書(アスキー出版局、1994年)P.248)

また外部データ伝送インターフェース部1/2:7/6とデータ伝送インターフェース部8間の通信回線の混雑状況に応じて送受信できる情報の転送レートが大きく影響を受ける。

【0093】このように外部との送受信情報をリアルタイムで情報記録媒体201に記録または情報記録媒体201からの再生をおこなう事は難しい。

【0094】図2のように外部との間で送受信する暗号化情報を外部伝送データ記憶部25に一時保管し、更に内部に持つ独自のクロックに従って暗号化情報を独立して作成する事により“プロトコル変換時の適応性”“外部通信回線混雑状況に対する柔軟性”を向上させている。

【0095】[4] ATAPI/SCSIコマンド

[4-1] 記憶装置の標準I/F

HDD、CD-ROM、DVD-ROM、MO、PD、MTなどコンピュータシステム内の記録装置に関する標準インターフェースとしてATAPIやSCSIが存在している。

【0096】各記憶装置とPCのメインCPU間ではATAPIやSCSIで決められたコマンドに従って情報の入出力や制御を行っている。

【0097】ATAPIおよびSCSI上で動く認証作業に関する標準コマンドとしては“リポートキーコマンド”と“センドキーコマンド”が存在している。

【0098】[4-2] コマンド形態

リポートキーコマンド/センドキーコマンドとも共通のコマンド形態として

◎“コマンド文”とその後に続く“データフォーマット”で構成される

◎コマンド文の中には“オペレーションコード”“AGID(オーセンティケーション グラント ID)”“キーフォーマット”が含まれる(AGIDに関する説明は後述する)と言う特徴がある。

【0099】[4-3] リポートキーコマンド

リポートキーコマンドとは認証相手2~5に情報を送信する時に使うコマンドでオペレーションコードは16進数で“A4”である。

【0100】○キーフォーマットが“000000”で“AGID”“ストリームID”“設定エリア情報”を送信し、

○キーフォーマットが“000001”で“チャレンジキー”を送信し、

○キーフォーマットが“000010”で“暗号化キー1”を送信する。

【0101】(“[5] 暗号鍵”で上記暗号鍵(各種キー)に付いての説明を行う)

[4-4] センドキーコマンド

センドキーコマンドとは認証相手2~5から情報を受信する時に使うコマンドでオペレーションコードは16進数で“A3”である。

【0102】○キーフォーマットが“000001”で“チャレンジキー”を送信し、

○キーフォーマットが“000011”で“暗号化キー2”を送信する。

【0103】(“[5] 暗号鍵”で上記暗号鍵(各種キー)に付いての説明を行う)

[5] 暗号鍵

[5-1] 暗号鍵の種類

図5に示すように一連の認証作業には“ストリームキー”“エリアキー”“チャレンジキー”“暗号化キー1”“暗号化キー2”“バスキー”の6種類の鍵が使われる。

【0104】[5-2] バスキー(暗号化して情報を送る際の共通鍵)

“[1-2] 複数の外部接続相手との間の情報伝送方法”で説明したように認証相手2~5に対して『暗号化情報の伝送』と『暗号化用の鍵の共有』を行っている。情報記録媒体201に記録する情報または情報記録媒体201から再生する情報の暗号化/復号化に用いられる暗号鍵を示す。上記暗号化部/復号化部/時変情報発生部23で用いられる。

【0105】暗号化技術は米国の輸出規制の対象になっている。現在RSA技術(暗号化方式の一つでアシンメトリックな公開鍵を用いる)では56ビット程度の暗号強度で有れば輸出可能であるが、それ以上のレンジでは輸出が難しい。また日本を対象とした米国輸出規制ではDES(暗号化方式の一つでシンメトリックな共通鍵を用いる)の暗号強度の限界を56ビットと定めている。同様にRC4やRC2(暗号化方式の一つでシンメトリックな共通鍵を用いる)の暗号強度の限界も56ビットと定めている。(杉本隆洋:イントラ&インターネットセキュリティ(オーム社1996年)P.1) 以上から米国の輸出規制を考慮に入れるとバスキーサイズは56ビットを標準に考える必要がある。しかし暗号鍵サイズが小さくなると大幅にセキュリティ確保(ハッカーによる暗号鍵の解読防止)が難しくなる。上記の状況を考えバスキーサイズは56ビットの半分である28ビット以上が望ましく、セキュリティ確保の観点から最低でも56ビットの1/4である14ビット以上は必要である。

【0106】[5-3] 暗号化キー1/2(バスキーを作るためのキー)

バスキーを作成するために、事前にバスキー作成の元になる鍵情報を相互に交換し合う。認証相手2～5に送信する鍵情報を“暗号化キー1”、認証相手2～5から受信する鍵情報を“暗号化キー2”と呼ぶ。認証相手2～5側と認証機能部9内で同一のルールに従って暗号化キー1と2を合成してバスキーを作成する。

【0107】上述した内容と同じ理由で暗号化キー1/2のサイズは28ビット以上が望ましく、最低でも14ビット以上は必要である。

【0108】【5-4】チャレンジキー（暗号化キー1/2を暗号化するためのキー）

暗号化キー1と2を生のまま送受信すると通信回線から傍受され、暗号化情報を容易に解読されてしまう。それを防止するため暗号化キー1と2自体を暗号化して伝送する。この暗号化キー1/2を暗号化するための暗号鍵をチャレンジキーと呼ぶ。

【0109】暗号化キー1/2を送受信する前に、通信回線を使ってチャレンジキーを相互交換する。

【0110】【5-5】ストリームキー（チャレンジキーを暗号化するためのキー）

セキュリティ確保のためチャレンジキーを用いても、チャレンジキー自体通信回線を使って伝送されるので、通信回線内の情報をすべて傍受していれば第三者が容易に暗号解読できる。さらにセキュリティ確保を強力にするため“ストリームキー”と“エリアキー”を使っている。

【0111】ストリームキーとは情報の種類毎に決められた暗号鍵の事を言う。例えば認証相手A2をMPEGエンコード/デコードボード、認証相手B3をオーディオエンコード/デコードボードとするとビデオストリームに対応したMPEGエンコード/デコードボードのみ共通の暗号鍵を事前に設定しておく。この暗号鍵情報は認証相手A2は知っているが、認証相手B3は知らない。従ってこの鍵で暗号化した情報を認証相手B3が傍受しても暗号を解読できない。

【0112】ストリームキーは図2の認証情報記憶部24にあらかじめ記憶されている。このストリームキーは情報内容に応じて対応する個々の認証相手2～5とそれぞれ共有化し、その情報は図6の情報a～d対応のストリームキー情報31～34としてあらかじめ記録されている。

【0113】【5-6】エリアキー（チャレンジキーを暗号化するためのキー）

例えばMPEGエンコード/デコードボードは情報記録再生装置1に直接接続されるPC（Personal Computer）だけでなく、ネットワークを介してつながっている他のPC（クライアント）の中にも装備されている。従ってストリームキーだけでは他のPC内のMPEGエンコード/デコードボードにより情報を傍受される危険性がある。それを回避するためエリアキーが存在する。

【0114】エリアキーとは

○情報記録再生装置1が直接接続されるPCシステムの範囲内

○TVやステレオなどのオーディオ・ビデオ機器も含めた個別システム（例えば1本のIEEE1394で接続されたシステム）の範囲内

○特定のファイアウォール（企業内LANの保護システム）内のローカルエリア（例えばファイアウォールで守られた1企業内、1学校内、1役所内、1地域内）の範囲内

○ワールドワイド領域に分類され、それぞれのエリアに応じて特定の共通鍵を持つ。エリアキーは事前に設定され、図6に示すように第1～4エリアキー情報31～34位置に記録されている。

【0115】エリアキーとストリームキーサイズは暗号化キー1/2のサイズの半分である。エリアキーとストリームキーをMSB、LSBとして並べてつなげたコードをチャレンジキーの暗号鍵として利用する。

【0116】従ってエリアキーとストリームキーサイズは上述した理由から14ビット以上が望ましく、最低でも5ビット以上は必要となる。

【0117】【6】1個の認証相手との間で行われる認証手順

【6-1】図5についての注釈

“【1-3】複数の外部接続相手との事前の認証作業”に示した事前の認証作業手順について図5を用いて詳細に説明する。

【0118】各認証相手2～5との間に行われる認証作業はATAPIもしくはSCSI上のコマンドの交換（リポートキーコマンドまたはセンドキーコマンド）により実施される。図5のフローチャートの各ステップの内、リポートキーコマンドによる送信に対応した部分を（RK）で表示し、センドキーコマンドによる受信に対応した部分を（SK）で示している。

【0119】【6-2】認証相手の設定

情報記録媒体201としてDVD-ビデオを用いた場合を例に取り、認証相手の設定方法について説明する。

【0120】情報記録媒体201の再生情報から情報の種類を判別するS101のステップでは“【2-4】DVD-ビデオにおける情報内容の識別方法”で説明したように図4のパケット12内に記録されているストリームIDもしくはサブストリームIDからパック10a～10d毎の情報種類を識別する。次に情報種類に応じてAGIDの割り付けS102を行う（詳細内容については“【7-2】同時並行認証方法”で説明する）。情報記録再生装置1が接続されているシステム規模に応じて認証処理制御部22で自動的に伝送対象エリアを設定S104し、それに対応したエリアキー情報35～38を認証情報記憶部24から再生し、そのアドレスを認証処理制御部22に通知する。更に上記識別した情報種類に

合わせてストリームキーを認証情報記憶部24から読み取りS105、そのアドレスを認証処理制御部22に通知する。

【0121】[6-3] 認証相手の探索と本人認証

この時点では認証相手A2～認証相手D5の内、どの相手が該当するか分からない。“[4-3] レポートキーコマンド”で説明したようにレポートキーコマンドを用いて全認証相手2～5に対して同時に“AGID”“ストリームID”“設定エリア情報”を送信する。

【0122】該当する認証相手A2は“ストリームID”と“設定エリア情報”から独自に“ストリームキー”と“エリアキー”を割り出し、その2個のキーをつなげて合成キーを作成し、その合成キーを用いて暗号化したチャレンジキーを送信するS107。

【0123】認証機能部9はこのチャレンジキーを受信すれば該当する認証相手A2の候補が存在する事を知る。またこれと平行して認証機能部9内部で独自に“ストリームキー”と“エリアキー”を割り出して合成キーを作成し、この合成キーを用いて暗号化したチャレンジキーの解読(復号化)を行う。正確に解読(復号化)出来れば送信相手が本物の認証相手A2で有ると分かる。

【0124】[6-4] チャレンジレスポンス

“[5] 暗号鍵”で説明した“暗号化キー1”“暗号化キー2”の送受信には暗号化した情報を送信し、受信側で復号化するステップを踏む。

【0125】暗号化技術において双方向本人認証方法として

OAからBへ特定情報を送る

OBはその情報を用いて暗号化した情報をAにもどす

OBから戻った情報から、Bが本人であることをAが確認する

OBからAへ特定情報を送る

OAはその情報を用いて暗号化した情報をBにもどす

OAから戻った情報から、Aが本人であることをBが確認すると言う方法が知られており、この方法を“チャレンジレスポンス”と言う。

【0126】認証機能部9でもこの“チャレンジレスポンス”を実施している。暗号化部/復号化部/時変情報発生部23で“暗号化キー1”を作成すると共に、それを認証相手A2から受信したチャレンジキーで暗号化して、認証相手A2に送信するS108。

【0127】次に暗号化部/復号化部/時変情報発生部23でチャレンジキーを作成し、それを“ストリームキー”と“エリアキー”から作成した合成キーを用いて暗号化して認証相手A2～認証相手D5に同時に送信するS109。“ストリームキー”と“エリアキー”を知っている本物の認証相手A2のみがこのチャレンジキーを解読できる。

【0128】認証相手A2は独自に“暗号化キー2”を作成し、受信したチャレンジキーを用いてそれを暗号化

して返信するS110。

【0129】[6-5] パスキー生成と暗号化情報伝送
この一連のステップにより得られた“暗号化キー1”と“暗号化キー2”から“パスキー”を生成するS111。この認証作業を完了させるとパスキーで伝送したい情報を暗号化し、“[3-7] 通信用プロトコル変換とタイミング確保”で説明したようにトランスポートストリームにプロトコル変換して伝送するS112。

【0130】[7] 複数の認証相手と行う同時並行認証方法

[7-1] 複数の認証相手との同時処理必要性

情報記録媒体201に記録/再生する情報は図3に示すようにバック毎に複数の情報種類が含まれている。また図2に示すように認証相手2～5が複数存在する。従って複数の認証相手2～5と同時に並行して認証作業および情報の伝送を行う必要がある。

【0131】[7-2] 同時並行認証方法

同時並行認証方法として別々の認証相手2～5と行う各認証ステップ(図5)毎に認証情報記憶部24に履歴を残す。

【0132】認証情報記憶部24内に記憶した履歴情報内容を図6に示す。認証機能部9では同時に4個の認証相手と認証作業および情報の伝送を行う事ができる。それぞれの認証作業毎にID番号(AGID)を割り当てて管理を行う。図6では各AGID番号40～43毎に認証履歴を縦方向(列方向)に記録する。

【0133】認証作業とその後に行われる情報の伝送処理が完了すると、対応するAGIDの列の情報をクリアし、AGID番号を解放する。

【0134】特定のAGID番号の処理が継続中に、新たな認証作業が発生すると認証処理制御部22は認証情報記憶部24内の空きAGID番号を探し、その列に認証履歴を記憶する。もし空きAGID番号が無い場合には認証不可能の情報をホストPCに通知するS103。このAGID番号の割り付けステップが図5のステップS102に相当する。

【0135】AGID番号40～43毎の認証履歴としては、相手が発行するチャレンジキー情報45～48、自分が発行するチャレンジキー情報51～54、自分が発行する暗号化キー1情報55～58、相手が発行する暗号化キー2情報60～63、パスキー情報65～68、AGID送信完了情報70～73、チャレンジキー受信完了情報75～78、暗号化キー1送信完了情報80～83、チャレンジキー送信完了情報85～88、暗号化キー2受信完了情報90～93からなっている。

【0136】[8] 認証作業時の具体的信号の流れ

[8-1] 認証処理制御部の内部構造

認証処理制御部22はCPUとそのCPUを制御するプログラムを記憶した半導体メモリ(RAM)から構成することが出来る。しかしここではより細かい信号の流れ

や機能を説明するため、認証処理制御部 22 を形成する各機能ブロック構成を図 7 に示し、演算処理部 100、演算実行プログラム解読部 101、算実行プログラムアドレス指定部 102、演算実行プログラム記憶部 103 から構成されている。

【0137】 [8-1-1] 演算実行プログラム記憶部 103 の機能

図 5 のフローチャートを実施するための演算実行プログラムが演算実行プログラム記憶部 103 に記憶されている。

【0138】 [8-1-2] 演算処理部 100 の機能

この演算実行プログラムに従って演算処理部 100 では
1) データ入出力インターフェース部 30 からの再生情報の伝送処理

データ入出力インターフェース部 30 への記録情報の伝送処理

2) 暗号化部/復号化部/時変情報発生部 23 での“暗号化処理”“復号化処理”“各種暗号鍵の作成処理”などの制御

3) 暗号化情報の外部伝送データ記憶部 25 への記憶処理

外部伝送データ記憶部 25 からの暗号化情報の再生処理などを行うと共に

4) 認証情報記憶部 24 に対する各種暗号鍵の一時保管や各ステップでの認証処理履歴の逐一保存をする事により複数の認証相手 2~5 との同時並行認証処理を可能にしている。

【0139】 [8-1-3] 演算実行プログラム解読部 101

演算実行プログラム記憶部 103 に記憶されている演算実行プログラムに対するプログラムコンパイルを演算実行プログラム解読部 101 内で行い、その結果を演算処理部 100 に伝送している。また演算実行プログラム解読部 101 では図 5 のフローチャートに従ったタイミング制御も行っている。

【0140】 [8-1-4] 演算実行プログラムアドレス指定部 102

複数の認証相手 2~5 との同時並行認証処理を行う場合、認証相手 2~5 毎に図 5 に示した認証ステップが異なる。例えば特定の時刻で見た場合、認証相手 A: 2 に対しては“認証相手 A: 2 に割付けた AGID 値の送信処理 S106”が完了し、認証相手 B: 3 ではすでに“こちら側のチャレンジキーで暗号化した“暗号化キー 2”の受信 S110”まで進み、認証相手 C: 4 には“認証相手 C: 4 から暗号化されたチャレンジキーを受信 S107”した所と言う場合がある。この直後に行う演算処理部 100 の処理は

a) 始めに認証相手 C: 4 に対して“認証相手 C: 4 のチャレンジキーで暗号化した“暗号化キー 1”を送信 S108”し、

b) 次に認証相手 B: 3 に対して“暗号化キー 1”と“暗号化キー 2”から“バスキー”を生成 S111 し、その結果を認証情報記憶部 24 に記憶した後でデータ入出力インターフェース部 30 から認証相手 B: 3 に対応した b パック 10b (図 3) 内のストリーム情報を読み込み、暗号化部/復号化部/時変情報発生部 23 で暗号化させて逐一外部伝送データ記憶部 25 に記憶する。

【0141】 c) “認証相手 A: 2 から暗号化されたチャレンジキーを受信 S107”したら上記の (b) の処理を中断して、“認証相手 A: 2 のチャレンジキーで暗号化した“暗号化キー 1”を送信 S108”する処理を行った後、“認証相手 A: 2 に暗号化されたこちら側のチャレンジキーを送信 S109”する処理を行う。その後上記の (b) の処理を継続する。

【0142】 上記の例から分かるように認証情報記憶部 24 に記憶した認証履歴に応じて複数の認証相手 2~5 に対して個々に図 5 のフローチャート上の異なるステップ処理を行う必要がある。上記の例を取れば、(a)~(c) のステップ毎に演算実行プログラム記憶部 103 上のプログラムが記憶されているアドレスが異なる。

(a) から (b)、(b) から (c) のステップにすぐに移行できるように演算実行プログラムアドレス指定部 102 によりジャンプするプログラムのアドレス指定を行っている。

【0143】 [8-2] 暗号化部/復号化部/時変情報発生部 23 の特徴

[8-2-1] 暗号化部/復号化部/時変情報発生部 23 の動作上の大きな特徴暗号化部/復号化部/時変情報発生部 23 は、図 8 に示すように、ランダム信号発生器 104、信号合成器 105、入出力信号切り替え制御器 106 から構成されている。

【0144】 暗号化部/復号化部/時変情報発生部 23 内で行う“情報の暗号化処理”“暗号化情報の復号化(暗号解読)処理”と“各種暗号鍵の基になる時変情報の発生”処理は、共に機能的に類似した処理を行っている。そのため上記の 3 つの処理を 1 組のランダム信号発生器 104 と信号合成器 105 で兼用している所に第 1 の大きな特徴を持つ。従来上記 3 つの処理を別々の回路を用いて行っていたのに対し、図 8 のように兼用化する事により大幅な回路の簡素化とその結果としての低価格化が達成できる。

【0145】 更にこのランダム信号発生器 104 を単なるシフトレジスタ 109a~d 列と見なして信号合成器 105 との組み合わせにより

◎ “エリアキー”と“ストリームキー”から“個々の認証相手との合成キー”の作成と

◎ “暗号化キー 1”と“暗号化キー 2”からの“バスキー”の合成を行っている所にも第 2 の特徴が有る。これにより同様に大幅な回路の簡素化とその結果としての低価格化が達成できる。

【0146】[8-2-2] ランダム信号発生器104 図8に示すようにシフトレジスタ109a~dと演算器108a、108bとセクタ107によりランダム信号発生器104が構成されている。

【0147】演算器108a、108bは排他的論理和回路である加算器から成る。セクタ107により演算器108aの出力信号i3がシフトレジスタ109aの入力i4に接続されている時はランダム信号発生器104を形成する。

【0148】すなわちシフトレジスタ109aの出力信号はシフトレジスタ109bの入力に入り、それが続いて信号がシフトレジスタ109dへ伝わる。シフトレジスタ109dの出力信号i5は演算器108bでシフトレジスタ109cの出力信号と加算され、その加算結果が更に演算器108aでシフトレジスタ109bの出力信号と加算され、その結果が再びシフトレジスタ109aに入力されて信号が循環する。この循環の結果、シフトレジスタ109dの出力信号i5はランダム信号になっている。このランダム信号発生器104の組み合わせを最適化すると“M系列のランダム信号発生器”になる。

【0149】[8-2-3] 信号合成器105 一般には信号合成器105は暗号化/復号化方式や“バスキー”作成方式に応じて複雑なゲートの組み合わせで構成される。但し、この信号合成器105は1個の排他的論理和回路である加算器のみで構成しても暗号化部/復号化部/時変情報発生部23としての機能は達成できる。

【0150】[8-3] 認証作業時の具体的信号の流れ 図5に示したフローチャートの各ステップでの具体的信号の流れに付いて以下に説明する。

【0151】1) ランダム信号発生器104の起動処理 情報記録再生装置1の電源を入れると認証処理制御部22の制御によりセクタ107にイニシャライズとして“0”の連続が送られる。“0”の連続の伝送がシフトレジスタ109内を一巡するとシフトレジスタ109dの出力i5が再度シフトレジスタ109aの入力i4に戻され、基準クロック発生器21の発生するクロックに同期して時変情報としてのランダム信号が発生する。

【0152】2) AGIDの割付け

図3に示した情報記録媒体201中に記録されたバック列の中から図4内のバケット12内のストリームIDとサブストリームIDを読み取り、必要なAGID数を調べる。認証処理制御部22では認証情報記憶部24内の“AGID送信完了情報70~73”を読み取り、空いている(まだ認証処理に使われてない)AGID番号を探す。各情報種類(ストリーム内容)毎にあいている所にAGIDを設定する。(以後、例として“AGID=0”の列を使って説明を行う。また認証相手として認証相手A:2が該当すると仮定する。)

3) エリアキーとストリームキーの設定

“[5-5] ストリームキー” “[5-6] エリアキー” “[6-2] 認証相手の設定”で説明した手順に従ってストリームキーとエリアキーを設定する。ストリームキーは認証情報記憶部24内の情報a~d対応のストリームキー情報31~34の中から選択し、エリアキーは認証情報記憶部24内の第1~4エリアキー情報35~38の中から選択する。

【0153】(以後、例として情報b対応のストリームキー情報32と第1エリアキー情報35を使った場合について説明する)

4) AGIDの送信処理

認証処理制御部22では設定したAGID番号とともに“ストリームID”と“設定エリア情報”をデータ伝送インターフェース部8に通知する。

【0154】通知が完了すると認証処理制御部22は認証情報記憶部24内のAGID送信完了情報70部分に“1”のビット(フラグ)を立てる。

【0155】データ伝送インターフェース部8では通知された“AGID番号” “ストリームID” “設定エリア情報”をATAPIまたはSCSIのレポートキーコマンドのフォーマットに合わせてフォーマット変更し、認証相手A:2に送信する。

【0156】5) 認証相手A:2からの暗号化されたチャレンジキーの受信

AGIDを受信すると認証相手A:2はチャレンジキーを発行し、ストリームキーとエリアキーから作った合成キーでそれを暗号化し、ATAPIまたはSCSIのSend Key Commandのフォーマットに合わせて送信する。

【0157】データ伝送インターフェース部8では暗号化された認証相手A:2が作成したチャレンジキーをATAPIまたはSCSIのセンドキーコマンドのフォーマットから抜き出し、外部伝送データ記憶部25に記憶する。

【0158】6) 時変情報の一時待避処理

認証相手A:2から受信したチャレンジキー復号化(解読)に先立ち、ランダム信号発生器104で発生する情報を認証情報記憶部24内に一時的に待避させる。すなわち認証処理制御部22からの指令で入出力信号切り替え制御器106はシフトレジスタ109d出力i5を直接取り込み、バスライン245を経由して認証情報記憶部24内の“ランダム信号発生器104で作られるタイムリーな時変情報39”(図6)に一時的に保存される。

【0159】7) 合成キー作成とチャレンジキーの復号化処理

演算実行プログラム記憶部103内のプログラムに従い、演算処理部100では認証情報記憶部24内の情報b対応のストリームキー情報32をバスライン26を経由して暗号化/復号化/時変情報発生部23へ伝送す

る。暗号化／復号化／時変情報発生部23内では入出力信号切り替え制御器106がセレクト107を制御して情報b対応のストリームキー情報32をそのままシフトレジスタ109aへ送る。その直後にそれに続いて認証情報記憶部24内の第1エリアキー情報35をシフトレジスタ109aへ送る。この時も前述した方法と同様な方法でシフトレジスタ109aへ送る。

【0160】第1エリアキー情報35をシフトレジスタ109aへ伝送完了時点で、情報b対応のストリームキー情報32の最初のビットがシフトレジスタ109dの最上位ビット位置に来ており、このシフトレジスタ109a～d内の情報が合成キーになる。

【0161】引き続き認証処理制御部22の制御により外部伝送データ記憶部25に記憶されている“暗号化されたチャレンジキー”が信号合成器105の入力信号i2として入力されるように入出力信号切り替え制御器106が働く。その結果、信号合成器105の出力信号i6に復号化（解読）されたチャレンジキーが現れる。その後、復号化（解読）されたチャレンジキー情報はシフトレジスタ110a～d、入出力信号切り替え制御器106、バスライン254を経由して認証情報記憶部24内の“相手が発行するチャレンジキー情報45”のアドレスに記憶される。

【0162】上記の説明では第1エリアキー情報35のシフトレジスタ109aへの伝送完了直後に暗号化されたチャレンジキーの復号化（解読）が開始されているが、それに限らずシフトレジスタ109aへの伝送完了後、特定のクロックを経た後で復号化を開始するように設定する事も可能である。

【0163】このように復号化後のチャレンジキーの認証情報記憶部24内への記憶が完了すると、チャレンジキー受信完了情報75のビット（フラグ）を“1”にする。

【0164】8）時変情報発生再開処理

AGID番号の暗号化処理が完了すると暗号化部／復号化部／時変情報発生部23は時変情報発生再開を行う。すなわち認証情報記憶部24内に一時的に保管されたランダム信号発生器で作られるタイムリーな時変情報39（図6）は認証処理制御部22の制御に応じてバスライン26、入出力信号切り替え制御器106、セレクト107を経てシフトレジスタ109aへ入力される（i4）。入力が完了するとセレクト107が閉じて演算器108aの出力信号i3をシフトレジスタ109の入力信号i4へ戻し、再び時変情報であるランダム信号を継続して発生させる。

【0165】9）暗号化キー1の作成

通常はランダム信号発生器104で常に時変情報を発生しているので、特定のタイミングでその時変情報を取り出す事により各種の暗号化鍵を作成できる。

【0166】演算実行プログラム記憶部103内のプロ

グラムに従い、演算処理部100の指令に応じてランダム信号発生器104の出力信号i5が“暗号化キー1”として入出力信号切り替え制御器106に入力され、バスライン26を経由して認証情報記憶部24内の“自分が発行する暗号化キー1情報55”（図6）に記憶される。暗号化キー1の記憶が完了すると“6）時変情報の一時待避処理”が行われる。

【0167】10）暗号化キー1の暗号化方法

認証処理制御部22の制御に従い、認証情報記憶部24内の“相手が発行するチャレンジキー情報45”のアドレスからチャレンジキーをバスライン26、入出力信号切り替え制御器106、セレクト107を経由してシフトレジスタ109aの入力部i4に入力される。入力が完了するとその信号が信号合成器105の入力部i5に入力される。

【0168】その後、セレクト107を閉じて特定クロック分だけランダム信号発生器104内を循環させた後、認証情報記憶部24内の“自分が発行する暗号化キー1情報55”のアドレスからバスライン26、入出力信号切り替え制御器106を経由してもう一方の信号合成器105の入力部i2に入力させる。信号合成器105の出力信号i6が暗号化された暗号化キー1となり、入出力信号切り替え制御器106バスライン26を経て外部伝送データ記憶部25に記憶される。

【0169】暗号化された暗号化キー1の作成が完了すると認証情報記憶部24内の“暗号化キー1送信完了情報80”のアドレスのビット（フラグ）を“1”にした後、“8）時変情報発生再開処理”に戻る。

【0170】11）暗号化キー1の送信処理

データ伝送インターフェース部8では外部伝送データ記憶部25から暗号化された暗号化キー1を読み取り、ATAPIまたはSCSIのレポートキーコマンドのフォーマットに合わせてフォーマット変更し、認証相手A：2に送信する。

【0171】12）チャレンジキーの送信処理

“9）暗号化キー1の作成”と同じ方法でチャレンジキーを作成し、“自分が発行するチャレンジキー情報50”のアドレスに保存する。次に“7）合成キー作成とチャレンジキーの復号化処理”と同じ方法で合成キーをシフトレジスタ109a～dにロードすると共に、チャレンジキーの暗号化を行う。

【0172】なお、同一の暗号鍵をシフトレジスタ109a～dにロードした場合、信号合成器105の入力i2に元の信号を入力すると出力信号i6として暗号化されると共に、信号合成器105の入力i2に暗号化された信号を入力すると出力信号i6として復号化（解読された）信号が得られる。暗号鍵信号として“0”にし“1”にし同じ信号を2回加算すると結果は元の信号に戻るため。

【0173】その後、暗号化されたチャレンジキーを外

部伝送データ記憶部 25 に記憶し、“チャレンジキー送信完了情報 85” のアドレスのビット（フラグ）を“1”にする。また“8”時変情報発生時の再開処理に戻る。

【0174】更に“11”暗号化キー 1 の送信処理”と同様にレポートキーコマンドで認証相手 A：2 に送信する。

【0175】13）バスキーの生成処理

“5）認証相手 A：2 からの暗号化されたチャレンジキーの受信”と同様に暗号化した“暗号化キー 2”を受信すると、“6）時変情報の一時待避処理”を行い、“10）暗号化キー 1 の暗号化方法”と同じ方法で“自分が発行するチャレンジキー情報 50”を用いて“暗号化キー 2”の復号化（解読）を行い、“相手が発行する暗号化キー 2 情報 60”アドレスに復号化後の暗号化キー 2 情報を記憶すると共に“暗号化キー 2 受信完了情報 90”のアドレスのビット（フラグ）を“1”にする。

【0176】次に認証情報記憶部 24 から“自分が発行する暗号化キー 1 情報”をバスライン 26、入出力信号切り替え制御器 106、セレクト 107 を経由してシフトレジスタ 109a～d の入力部 i 4 へ入力させる。ここでシフトレジスタ 109a～d は“自分が発行する暗号化キー 1 情報”の一時保存場所として使用している。

【0177】“自分が発行する暗号化キー 1 情報”がシフトレジスタ 109d まで埋まると“相手が発行する暗号化キー 2 情報”をバスライン 26、入出力信号切り替え制御器 106 経由で信号合成器 105 の入力部 i 2 に入力し、信号合成器 105 で暗号化キー 1 と暗号化キー 2 の合成を行う。信号合成器 105 出力信号 i 6 がバスキーとなり、認証情報記憶部 24 内の“バスキー情報 65”のアドレスに記憶される。

【0178】14）再生情報の暗号化処理

情報記録媒体 201 から再生した情報を暗号化して送信する場合、認証処理制御部 22 の制御に従い、次に認証情報記憶部 24 から“バスキー情報 65”をバスライン 26、入出力信号切り替え制御器 106、セレクト 107 を経由してシフトレジスタ 109 の入力部 i 4 へ入力させる。バスキーの転送が完了するとセレクト 107 が閉じ、バスキーを出発点として信号がランダム信号発生器 104 内で循環する。再生信号の暗号化が続く限りこの循環は継続される。

【0179】情報記録媒体 201 から再生した情報はデータ入出力インターフェース部 30 からバスライン 26、入出力信号切り替え器 106 を経て信号合成器 105 の入力部 i 2 に入力され、信号合成器 105 出力である暗号化された情報は i 6 からシフトレジスタ 110a～d、入出力信号切り替え器 106、バスライン 26 を経て外部伝送データ記憶部 25 へ記憶される。

【0180】15）複数認証相手との並行処理、割り込み処理

以上 1 個の認証相手 A：2 との間の認証手続きについて説明した。上述の説明から明らかなように、各ステップ毎に認証履歴を認証情報記憶部 25 に記憶して有るので途中で認証手続きを中断し、他の認証相手 B：3 との認証手続きを行うことが出来る。

【0181】[9] ネットワークを用いた認証処理方法
[9-1] TCP/IP を用いた場合のネットワーク上認証処理

ネットワークシステム上での認証方法については“[1-4] ネットワークシステムにおける情報伝送の具体例”で説明した。ここでは図 5 に示した認証手順フローチャートの各ステップとネットワーク上の通信内容との対応を通信プロトコルとして TCP/IP を例にとりて説明する。

【0182】“[8] 認証作業時の具体的信号の流れ”では情報記録媒体 201 の再生情報から認証処理が開始されるが、ネットワーク上の認証処理では“[1-4] ネットワークシステムにおける情報伝送の具体例”で説明したようにネットワークサーバから情報の配送・収集先のクライアント（の IP アドレスや電話番号）と配送・収集する情報内容を通知されて初めて認証処理を開始する。

【0183】[9-2] サーバから特定のクライアントを指定された場合

この場合にはクライアントから特定の IP アドレスや接続先の電話番号を指定されるので認証相手 A：2 は事前に固定される。従って図 5 の“認証相手に割付けた AGID の値・エリア情報・ストリーム ID 情報の送信 S106”は事前に固定された相手に対して行われる。この場合にはそれ以降の各ステップは情報伝送時の漏洩防止・セキュリティ確保のための暗号キーの共有化処理となる。具体的な処理内容は“[8-3] 認証作業時の具体的信号の流れ”と同じになる。

【0184】ネットワークを用いて相手のクライアントに情報を送信するまたはクライアントから情報を受信する場合、経路途中のゲートウェイ（ルーター）で伝送する情報を容易にコピーできる。従って漏洩防止・セキュリティ確保のため共有化した暗号キーを用いて暗号化した情報を伝送する事が非常に重要となる。

【0185】[9-3] サーバから同時に複数のクライアントを指定された場合

電子メールを使って複数のクライアントに多量の情報を送付するような場合、サーバから同時に複数のクライアントを指定される事が有る。伝送する情報が機密性の高い場合には個々のクライアントをそれぞれ別々の認証相手 A：2～D：5 と考え、個々に通信して認証作業を行う。それ以外は“[9-1-1] サーバから特定のクライアントを指定された場合”と同じ処理になる。[9-4] サーバからクライアント範囲のみを指定された場合 TCP/IP プロトコルの場合、サーバは自分が通信を

行うクライアントのIPアドレスとクライアントマシン名の一覧表を“hosts”と言う名のファイルに保存している。またサーバが管理するネットワークドメインを持ち、そのドメインに含まれるクライアントマシンをIPアドレス等で管理している。サーバから情報記録再生装置に対して情報伝送相手のクライアントを指定する代わりに情報を送信するあるいは情報を受信するクライアントの範囲を指定して、その中から該当クライアントを探し、情報を送受信するように要求される場合がある。この時サーバから情報記録再生装置に対して示されるクライアントの範囲として“hosts”そのものを渡したり、特定のドメインに含まれるクライアントマシンのIPアドレスリストを渡す。

【0186】図5“認証相手が属するエリアに応じた該当エリアキーの設定S104”はサーバから通知されたネットワークドメインの認識と、ネットワークドメイン毎に事前に設定して有る暗号鍵であるエリアキーの抽出に対応する。ネットワークドメインに対する対応するエリアキーの情報は図2の認証情報記憶部24に事前に記憶して有る。

【0187】認証機能部9では通信機能を有するデータ伝送インターフェース部8を制御してIPアドレスリストに含まれる全クライアントに対して同時に図5の“認証相手に割付けたAGIDの値・エリア情報・ストリームID情報の送信S106”を送信する。送信する情報によってはクライアントに対してストリームID情報の代わりに別のフォーマットに基付いたこれから伝送しようとしている情報内容に関する情報を伝送する場合もある。このステップを実施するとネットワーク内の情報配送を受けたいクライアント、もしくは情報送信する必要があるクライアントから“自己申請”の形で回答が来る。すなわち該当クライアントである“認証相手から暗号化されたチャレンジキーを受信するS107”の形で回答が来る。TCP/IPプロトコルでは必ず通信パケット内に送信側のIPアドレスが含まれるので、認証処理制御部22はその受信した通信パケットから認証相手A:2のIPアドレスを取り出して、図2の認証情報記憶部24に保存する。以後保存したIPアドレスを用いて認証相手A:2との認証作業を行う。つまり“認証相手のチャレンジキーで暗号化した“暗号化キー1”を送信S108”以降の全ステップは上記に抽出したIPアドレスを持ったクライアントに対してのみ通信を行う。

【0188】“認証相手に割付けたAGIDの値・エリア情報・ストリームID情報の送信S106”に対して複数のクライアントが該当し、複数のクライアントから回答が来た場合には、ここのクライアントをそれぞれ異なる認証相手B:3、認証相手C:4、認証相手D:5と分けて個々に認証作業を行う。

【0189】ネットワーク経路途中での情報の不正コピー、情報漏洩を防止し、セキュリティを確保するため

に個々のクライアント毎に異なる認証相手と見なして別々に認証作業を行う事が望ましい。

【0190】図5“認証相手のチャレンジキーで暗号化した“暗号化キー1”を送信S108”以降の認証処理の具体的内容は“[8-3] 認証作業時の具体的信号の流れ”と基本的に同じ処理となる。

【0191】図9を用いて情報記録再生装置1内の情報記録再生部（物理系ブロック）200の内部構造を説明する。

【0192】[10] 情報記録再生部200の機能説明
[10-1] 情報記録再生部200の基本機能
情報記録再生部200では

◎情報記録媒体201上の所定位置に集光スポットを用いて新規情報の記録あるいは書き換え（情報の消去も含む）を行う。

【0193】◎情報記録媒体201上の所定位置から集光スポットを用いてすでに記録されている情報の再生を行う。

【0194】の処理を行う。

【0195】[10-2] 情報記録再生部200の基本機能達成手段

上記の基本機能を達成する手段として情報記録再生部200では

◎情報記録媒体201上のトラック（図示して無い）に沿って集光スポットをトレース（追従）させる。

【0196】◎情報記録媒体201に照射する集光スポットの光量を変化させて情報の記録／再生／消去の切り替えを行う。

【0197】◎外部から与えられる記録信号dを高密度かつ低エラー率で記録するために最適な信号に変換する。

【0198】を行っている。

【0199】[11] 機構部分の構造と検出部分の動作
[11-1] 光学ヘッド202基本構造と信号検出回路
[11-1-1] 光学ヘッド202による信号検出
光学ヘッド202は基本的には図示して無いが光源である半導体レーザ素子と光検出器と対物レンズから構成されている。

【0200】半導体レーザ素子から発光されたレーザ光は対物レンズにより情報記録媒体（光ディスク）201上に集光される。情報記録媒体（光ディスク）201の光反射膜もしくは光反射性記録膜で反射されたレーザ光は光検出器により光電変換される。

【0201】光検出器で得られた検出電流はアンプ213により電流-電圧変換されて検出信号となる。この検出信号はフォーカス・トラックエラー検出回路217あるいは2値化回路212で処理される。一般的には光検出器は複数の光検出領域に分割され、各光検出領域に照射される光量変化を個々に検出している。この個々の検出信号に対してフォーカス・トラックエラー検出回路2

17で和・差の演算を行いフォーカスずれとトラックずれの検出を行う。情報記録媒体（光ディスク）201の光反射膜もしくは光反射性記録膜からの反射光量変化を検出して情報記録媒体201上の信号を再生する。

【0202】[11-1-2]フォーカスずれ検出方法
フォーカスずれ量を光学的に検出する方法として

○非点収差法：情報記録媒体（光ディスク）201の光反射膜もしくは光反射性記録膜で反射されたレーザ光の検出光路に図示して無いが非点収差を発生させる光学素子を配置し、光検出器上に照射されるレーザ光の形状変化を検出する方法。光検出領域は対角線状に4分割されている。各検出領域から得られる検出信号に対し、フォーカス・トラックエラー検出回路217内で対角和間の差を取ってフォーカスエラー検出信号を得る。あるいは

○ナイフエッジ法：情報記録媒体201で反射されたレーザ光に対して非対称に一部を遮光するナイフエッジを配置する方法。光検出領域は2分割され、各検出領域から得られる検出信号間の差を取ってフォーカスエラー検出信号を得る。のどちらかを使う場合が多い。

【0203】[11-1-3]トラックずれ検出方法
情報記録媒体（光ディスク）201はスパイラル状または同心円状のトラックを有し、トラック上に情報が記録される。このトラックに沿って集光スポットをトレースさせて情報の再生もしくは記録／消去を行う。安定して集光スポットをトラックに沿ってトレースさせるため、トラックと集光スポットの相対的位置ずれを光学的に検出する必要がある。トラックずれ検出方法としては一般に

○DPD(Differential Phase Detection)法：情報記録媒体（光ディスク）201の光反射膜もしくは光反射性記録膜で反射されたレーザ光の光検出器上での強度分布変化を検出する。光検出領域は対角線状に4分割されている。各検出領域から得られる検出信号に対し、フォーカス・トラックエラー検出回路217内で対角和間の差を取ってトラックエラー検出信号を得る。あるいは

○プッシュプル法：情報記録媒体201で反射されたレーザ光の光検出器上での強度分布変化を検出する。光検出領域は2分割され、各検出領域から得られる検出信号間の差を取ってトラックエラー検出信号を得る。

【0204】○ツインスポット法：半導体レーザ素子と情報記録媒体201間の送光系に回折素子などを配置して光を複数に波面分割し、情報記録媒体201上に照射する±1次回折光の反射光量変化を検出する。再生信号検出用の光検出領域とは別に+1次回折光の反射光量と-1次回折光の反射光量を個々に検出する光検出領域を配置し、それぞれの検出信号の差を取ってトラックエラー検出信号を得る。などが有る。

【0205】[11-1-4]対物レンズアクチュエー

タ構造

半導体レーザ素子から発光されたレーザ光を情報記録媒体201上に集光させる対物レンズ（図示されて無い）は対物レンズアクチュエータ駆動回路218の出力電流に応じて2軸方向に移動可能な構造になっている。この対物レンズの移動方向は

・フォーカスずれ補正用に情報記録媒体201に対する垂直方向に移動し、

・トラックずれ補正用に情報記録媒体201の半径方向に移動する。

【0206】図示して無いが対物レンズの移動機構を対物レンズアクチュエータと呼ぶ。対物レンズアクチュエータ構造としては

○軸摺動方式：中心軸（シャフト）に沿って対物レンズと一体のブレードが移動する方式で、ブレードが中心軸に沿った方向に移動してフォーカスずれ補正を行い、中心軸を基準としたブレードの回転運動によりトラックずれ補正を行う方法あるいは

○4本ワイヤー方式：対物レンズ一体のブレードが固定系に対し4本のワイヤで連結されており、ワイヤーの弾性変形を利用してブレードを2軸方向に移動させる方法が多く使われている。いずれの方式も永久磁石とコイルを持ち、ブレードに連結したコイルに電流を流す事によりブレードを移動させる構造になっている。

【0207】[11-2]情報記録媒体201の回転制御系

スピンドルモータ204の駆動力によって回転する回転テーブル221上に情報記録媒体（光ディスク）201を装着する。

【0208】情報記録媒体201の回転数は情報記録媒体201から得られる再生信号によって検出する。すなわちアンプ213出力の検出信号（アナログ信号）は2値化回路212でデジタル信号に変換され、この信号からPLL回路211により一定周期信号（基準クロック信号）を発生させる。情報記録媒体回転速度検出回路214ではこの信号を用いて情報記録媒体201の回転数を検出し、その値を出力する。

【0209】情報記録媒体201上で再生あるいは記録／消去する半径位置に対応した情報記録媒体回転数の対応テーブルは半導体メモリ219にあらかじめ記録して有る。再生位置もしくは記録／消去位置が決まると、制御部220は半導体メモリ219情報を参照して情報記録媒体201の目標回転数を設定し、その値をスピンドルモータ駆動回路215に通知する。

【0210】スピンドルモータ駆動回路215では、この目標回転数と情報記録媒体回転速度検出回路214の出力信号（現状での回転数）との差を求め、その結果に応じた駆動電流をスピンドルモータ204に与えてスピンドルモータ204の回転数が一定になるように制御する。情報記録媒体回転速度検出回路214の出力信号は

情報記録媒体 201 の回転数に対応した周波数を有するパルス信号で、スピンドルモータ駆動回路 215 ではこの信号の周波数とパルス位相の両方に対して制御する。

【0211】 [11-3] 光学ヘッド移動機構

情報記録媒体 201 の半径方向に光学ヘッド 202 を移動させるため光学ヘッド移動機構（送りモータ）203 を持っている。

【0212】 光学ヘッド 202 を移動させるガイド機構として棒状のガイドシャフトを利用する場合が多く、このガイドシャフトと光学ヘッド 202 の一部に取り付けられたブッシュ間の摩擦を利用して光学ヘッド 202 が移動する。それ以外に回転運動を使用して摩擦力を軽減させたベアリングを用いる方法も有る。

【0213】 光学ヘッド 202 を移動させる駆動力伝達方法は図示して無いが固定系にピニオン（回転ギヤ）の付いた回転モータを配置し、ピニオンとかみ合う直線状のギヤであるラックを光学ヘッド 202 の側面に配置して回転モータの回転運動を光学ヘッド 202 の直線運動に変換している。それ以外の駆動力伝達方法としては固定系に永久磁石を配置し、光学ヘッド 202 に配置したコイルに電流を流して直線方向に移動させるリニアモータ方式を使う場合もある。

【0214】 回転モータ、リニアモータいずれの方式でも基本的には送りモータに電流を流して光学ヘッド 202 移動用の駆動力を発生させている。この駆動用電流は送りモータ駆動回路 216 から供給される。

【0215】 [12] 各制御回路の機能

[12-1] 集光スポットトレース制御

フォーカスずれ補正あるいはトラックずれ補正を行うため、フォーカス・トラックエラー検出回路 217 の出力信号（検出信号）に応じて光学ヘッド 202 内の対物レンズアクチュエータ（図示して無い）に駆動電流を供給する回路が対物レンズアクチュエータ駆動回路 218 である。高い周波数領域まで対物レンズ移動を高速度応答させるため、対物レンズアクチュエータの周波数特性に合わせた特性改善用の位相補償回路を内部に有している。

【0216】 対物レンズアクチュエータ駆動回路 218 では制御部 220 の命令に応じて

◎フォーカス／トラックずれ補正動作（フォーカス／トラックループ）の ON/OFF 処理

◎情報記録媒体 201 の垂直方向（フォーカス方向）へ対物レンズを低速で移動させる処理（フォーカス／トラックループ OFF 時に実行）

◎キックパルスを用いて情報記録媒体 201 の半径方向（トラックを横切る方向）にわずかに動かして、集光スポットを隣のトラックへ移動させる処理を行う。

【0217】 [12-2] レーザ光量制御

[12-2-1] 再生と記録／消去の切り替え処理

再生と記録／消去の切り替えは情報記録媒体 201 上に照射する集光スポットの光量を変化させて行う。

【0218】 相変化方式を用いた情報記録媒体に対しては一般的に

〔記録時の光量〕 > 〔消去時の光量〕 > 〔再生時の光量〕

の関係が成り立ち、光磁気方式を用いた情報記録媒体に対しては一般的に

〔記録時の光量〕 〔消去時の光量〕 > 〔再生時の光量〕

の関係が有る。光磁気方式の場合には記録／消去時には情報記録媒体 201 に加える外部磁場（図示して無い）の極性を変えて記録と消去の処理を制御している。

【0219】 情報再生時には情報記録媒体 201 上には一定の光量を連続的に照射している。

【0220】 新たな情報を記録する場合には、この再生時の光量の上にパルス状の断続的光量を上乗せする。半導体レーザ素子が大きな光量でパルス発光した時に情報記録媒体 201 の光反射性記録膜が局所的に光学的变化もしくは形状変化を起こし、記録マークが形成される。すでに記録されている領域の上に重ね書きする場合も同様に半導体レーザ素子をパルス発光させる。

【0221】 すでに記録されている情報を消去する場合には、再生時よりも大きな一定光量を連続照射する。連続的に情報を消去する場合にはセクター単位など特定周期毎に照射光量を再生時に戻し、消去処理と平行して間欠的に情報再生を行う。間欠的に消去するトラックのトラック番号やアドレスを再生し、消去トラックの誤りが無い事を確認しながら消去処理を行っている。

【0222】 [12-2-2] レーザ発光制御

図示して無いが光学ヘッド 202 内には半導体レーザ素子の発光量を検出するための光検出器を内蔵している。半導体レーザ駆動回路 205 ではその光検出器出力（半導体レーザ素子発光量の検出信号）と記録／再生／消去制御波形発生回路 206 から与えられる発光基準信号との差を取り、その結果に基づき半導体レーザへの駆動電流をフィードバックしている。

【0223】 [13] 機構部分の制御系に関する諸動作 [13-1] 起動制御

情報記録媒体（光ディスク）201 を回転テーブル 221 上に装着し、起動制御を開始すると、以下の手順に従って処理が行われる。

【0224】 1) 制御部 220 からスピンドルモータ駆動回路 215 に目標回転数が伝えられ、スピンドルモータ駆動回路 215 からスピンドルモータ 204 に駆動電流が供給されてスピンドルモータ 204 の回転が開始する。

【0225】 2) 同時に制御部 220 から送りモータ駆動回路 216 に対してコマンド（実行命令）が出され、送りモータ駆動回路 216 から光学ヘッド駆動機構（送りモータ）203 に駆動電流が供給されて光学ヘッド 202 が情報記録媒体 201 の最内周位置に移動する。情

報記録媒体201の情報が記録されている領域を越えてさらに内周部に光学ヘッド202が来ている事を確認する。

【0226】3) スピンドルモータ204が目標回転数に到達すると、そのステータス(状況報告)が制御部220に出される。

【0227】4) 制御部220から記録/再生/消去制御波形発生回路206に送られた再生光量信号に合わせて半導体レーザ駆動回路205から光学ヘッド202内の半導体レーザ素子に電流が供給されてレーザ発光を開始する。

【0228】*情報記録媒体(光ディスク)201の種類によって再生時の最適照射光量が異なる。起動時にはそのうちの最も照射光量の低い値に設定する。

【0229】5) 制御部220からのコマンドに従って光学ヘッド202内の対物レンズ(図示して無い)を情報記録媒体201から最も遠ざけた位置にずらし、ゆっくりと対物レンズを情報記録媒体201に近付けるよう対物レンズアクチュエータ駆動回路218が制御する。

【0230】6) 同時にフォーカス・トラックエラー検出回路217でフォーカスずれ量をモニターし、焦点が合った位置近傍に対物レンズが来た時ステータスを出して制御部220に通知する。

【0231】7) 制御部220ではその通知をもらって、対物レンズアクチュエータ駆動回路218に対してフォーカスループをオンにするようコマンドを出す。

【0232】8) 制御部220はフォーカスループをオンにしたまま送りモータ駆動回路216にコマンドを出して光学ヘッド202をゆっくり情報記録媒体201の外周部方向へ移動させる。

【0233】9) 同時に光学ヘッド202からの再生信号をモニターし、光学ヘッド202が情報記録媒体201上の記録領域に到達したら光学ヘッド202の移動を止め、対物レンズアクチュエータ駆動回路218に対してトラックループをONさせるコマンドを出す。

【0234】10) 情報記録媒体(光ディスク)201の内周部に記録されている“再生時の最適光量”と“記録/消去時の最適光量”を再生し、その情報が制御部220を経由して半導体メモリ219に記録される。

【0235】11) さらに制御部220ではその“再生時の最適光量”に合わせた信号を記録/再生/消去制御波形発生回路206に送り、再生時の半導体レーザ素子の発光量を再設定する。

【0236】12) 情報記録媒体201に記録されている“記録/消去時の最適光量”に合わせて記録/消去時の半導体レーザ素子の発光量が設定される。

【0237】[13-2] アクセス制御

[13-2-1] 情報記録媒体201上のアクセス先情報の再生

情報記録媒体201上のどの場所にどのような内容の情

報が記録されているかに付いての情報は情報記録媒体201の種類により異なり、一般的には情報記録媒体201内の

◎ディレクトリ管理領域: 情報記録媒体201の内周領域もしくは外周領域にまとまって記録して有る

かまたは

◎ナビゲーションバック: MPEG2のPS(プログラム ストリーム)のデータ構造に準拠したVOBS(ビデオ オブジェクト セット)の中に含まれ、次の映像がどこに記録して有るかの情報が記録されているなどに記録して有る。

【0238】特定の情報を再生あるいは記録/消去したい場合には、まず上記の領域内の情報を再生し、そこで得られた情報からアクセス先を決定する。

【0239】[13-2-2] 粗アクセス制御
制御部220ではアクセス先の半径位置を計算で求め、現状の光学ヘッド202位置との間の距離を割り出す。

【0240】光学ヘッド202移動距離に対して最も短時間で到達出来る速度曲線情報が事前に半導体メモリ219内に記録されている。制御部220はその情報を読み取り、その速度曲線に従って以下の方法で光学ヘッド202の移動制御を行う。

【0241】制御部220から対物レンズアクチュエータ駆動回路218に対してコマンドを出してトラックループをOFFした後、送りモータ駆動回路216を制御して光学ヘッド202の移動を開始させる。

【0242】集光スポットが情報記録媒体201上のトラックを横切ると、フォーカス・トラックエラー検出回路217内でトラックエラー検出信号が発生する。このトラックエラー検出信号を用いて情報記録媒体201に対する集光スポットの相対速度が検出できる。

【0243】送りモータ駆動回路216では、このフォーカス・トラックエラー検出回路217から得られる集光スポットの相対速度と制御部220から逐一送られる目標速度情報との差を演算し、その結果を光学ヘッド駆動機構(送りモータ)203への駆動電流にフィードバックかけながら光学ヘッド202を移動させる。

【0244】“[11-3] 光学ヘッド移動機構”に記述したようにガイドシャフトとブッシュあるいはベアリング間には常に摩擦力が働いている。光学ヘッド202が高速に移動している時は動摩擦が働くが、移動開始時と停止直前には光学ヘッド202の移動速度が遅いため静止摩擦が働く。この時には相対的摩擦力が増加しているので(特に停止直前には)制御部220からのコマンドに応じて光学ヘッド駆動機構(送りモータ)203に供給する電流の増幅率(ゲイン)を増加させる。

【0245】[13-2-3] 密アクセス制御
光学ヘッド202が目標位置に到達すると制御部220から対物レンズアクチュエータ駆動回路218にコマンドを出してトラックループをONさせる。

【0246】集光スポットは情報記憶媒体201上のトラックに沿ってトレースしながらその部分のアドレスもしくはトラック番号を再生する。

【0247】そこでのアドレスもしくはトラック番号から現在の集光スポット位置を割り出し、到達目標位置からの誤差トラック数を制御部220内で計算し、集光スポットの移動に必要なトラック数を対物レンズアクチュエータ駆動回路218に通知する。

【0248】対物レンズアクチュエータ駆動回路218内で1組キックパルスを発生させると対物レンズは情報記憶媒体201の半径方向にわずかに動いて、集光スポットが隣のトラックへ移動する。

【0249】対物レンズアクチュエータ駆動回路218内では一時的にトラックループをOFFさせ、制御部220からの情報に合わせた回数のキックパルスを発生させた後、再びトラックループをONさせる。

【0250】密アクセス終了後、制御部220は集光スポットがトレースしている位置の情報（アドレスもしくはトラック番号）を再生し、目標トラックにアクセスしている事を確認する。

【0251】【13-3】連続記録／再生／消去制御
図9に示すようにフォーカス・トラックエラー検出回路217から出力されるトラックエラー検出信号は送りモータ駆動回路216に入力されている。上述した“起動制御時”と“アクセス制御時”には送りモータ駆動回路216内ではトラックエラー検出信号を使用しないように制御部220により制御されている。

【0252】アクセスにより集光スポットが目標トラックに到達した事を確認した後、制御部220からのコマンドによりモータ駆動回路216を経由してトラックエラー検出信号の一部が光学ヘッド駆動機構（送りモータ）203への駆動電流として供給される。連続に再生もしくは記録／消去処理を行っている期間中、この制御は継続される。

【0253】情報記憶媒体201の中心位置は回転テーブル221の中心位置とわずかにずれた偏心を持って装着されている。トラックエラー検出信号の一部を駆動電流として供給すると、偏心に合わせて光学ヘッド202全体が微動する。

【0254】また長時間連続して再生もしくは記録／消去処理を行うと、集光スポット位置が徐々に外周方向もしくは内周方向に移動する。トラックエラー検出信号の一部を光学ヘッド移動機構（送りモータ）203への駆動電流として供給した場合には、それに合わせて光学ヘッド202が徐々に外周方向もしくは内周方向に移動する。

【0255】このようにして対物レンズアクチュエータのトラックずれ補正の負担を軽減し、トラックループを安定化出来る。

【0256】【13-4】終了制御

一連の処理が完了し、動作を終了させる場合には以下の手順に従って処理が行われる。

【0257】1) 制御部220から対物レンズアクチュエータ駆動回路218に対してトラックループをOFFさせるコマンドが出される。

【0258】2) 制御部220から対物レンズアクチュエータ駆動回路218に対してフォーカスループをOFFさせるコマンドが出される。

【0259】3) 制御部220から記録／再生／消去制御波形発生回路206に対して半導体レーザ素子の発光を停止させるコマンドが出される。

【0260】4) スピンドルモータ駆動回路215に対して基準回転数として0を通知する。

【0261】【14】情報記憶媒体への記録信号／再生信号の流れ

【14-1】情報記憶媒体201に記録される信号形式
情報記憶媒体201上に記録する信号に対して

◎情報記憶媒体201上の欠陥に起因する記録情報エラーの訂正を可能とする

◎再生信号の直流成分を0にして再生処理回路の簡素化を図る

◎情報記憶媒体201に対して出来るだけ高密度に情報を記録するとの要求を満足するため図9に示すように情報記録再生部（物理系ブロック）200では“エラー訂正機能の付加”“記録情報に対する信号変換（信号の変復調）”を行っている。

【0262】【14-2】記録時の信号の流れ

【14-2-1】ECC (Error Correction Code) 付加処理

情報記憶媒体201に記録したい情報が生信号の形で記録信号dとしてデータ入出力インターフェース部30に入力される。この記録信号dはそのまま半導体メモリ219に記録され、その後ECCエンコーディング回路208で以下のようにECCの付加処理を実行する。

【0263】以下に積符号を用いたECC付加方法の実施例について説明する。

【0264】記録信号dは半導体メモリ219内で172Bytes 毎に1行ずつ順次並べ、192行で1組のECCブロックとする。この“行:172×列:192Bytes”で構成される1組のECCブロック内の生信号（記録信号d）に対し、172Bytesの1行毎に10Bytes の内符号PIを計算して半導体メモリ219内に追加記録する。さらに Bytes 単位の1列毎に16Bytes の外符号POを計算して半導体メモリ219内に追加記録する。

【0265】情報記憶媒体201に記録する実施例としては内符号PIを含めた12行と外符号PO分1行の合計2366Bytes

$(2366 = (12 + 1) \times (172 + 10))$

を単位として情報記憶媒体の1セクター内に記録する。

【0266】ECCエンコーディング回路208では内

符号P Iと外符号P Oの付加が完了すると、半導体メモリ219から1セクター分の2366Bytes ずつの信号を読み取り、変調回路207へ転送する。

【0267】[14-2-2] 信号変調

再生信号の直流成分(DSV:Disital Sum Value)を0に近付け、情報記憶媒体201に対して高密度に情報を記録するため、信号形式の変換である信号変調を変調回路207内で行う。

【0268】元の信号と変調後の信号との間の関係を示す変換テーブルを変調回路207と復調回路210内部で持っている。ECCエンコーディング回路208から転送された信号を変調方式に従って複数ビット毎に区切り、変換テーブルを参照しながら別の信号(コード)に変換する。

【0269】例えば変調方式として8/16変調(RLL(2,10)コード)を用いた場合には、変換テーブルが2種類存在し、変調後の直流成分(DSV:Disital SumValue)が0に近づくように逐一参照用変換テーブルを切り替えている。

【0270】[14-2-3] 記録波形発生

情報記憶媒体(光ディスク)201に記録マークを記録する場合、一般的には記録方式として

○マーク長記録方式:記録マークの前端位置と後端末位置に“1”が来る。と

○マーク間記録方式:記録マークの中心位置が“1”の位置と一致する。

【0271】の2種類存在する。

【0272】またマーク長記録を行った場合、長い記録マークを形成する必要がある。この場合、一定期間記録光量を照射し続けると情報記憶媒体201の光反射性記録膜の蓄熱効果により後部のみ幅が広い“雨だれ”形状の記録マークが形成される。この弊害を除去するため、長さの長い記録マークを形成する場合には複数の記録パルスに分割したり、記録波形を階段状に変化させている。

【0273】記録/再生/消去制御波形発生回路206内では変調回路207から送られて来た記録信号に応じて上記のような記録波形を作成し、半導体レーザ駆動回路205に伝達している。

【0274】[14-3] 再生時の信号の流れ

[14-3-1] 2値化・PLL回路

“[11-1-1] 光学ヘッド202による信号検出”で記述したように情報記憶媒体(光ディスク)201の光反射膜もしくは光反射性記録膜からの反射光量変化を検出して情報記憶媒体201上の信号を再生する。アンブ213で得られた信号はアナログ波形をしている。2値化回路212ではその信号をコンパレータを用いて“1”と“0”からなる2値のデジタル信号に変換する。

【0275】ここから得られた再生信号からPLL回路

211で情報再生時の基準信号を取り出している。PLL回路211は周波数可変の発振器を内蔵している。その発振器から出力されるパルス信号(基準クロック)と2値化回路212出力信号間の周波数と位相の比較を行い、その結果を発振器出力にフィードバックしている。

【0276】[14-3-2] 信号の復調

変調された信号と復調後の信号との間の関係を示す変換テーブルを復調回路210内部で持っている。PLL回路211で得られた基準クロックに合わせて変換テーブルを参照しながら信号を元の信号に戻す。戻した(復調した)信号は半導体メモリ219に記録される。

【0277】[14-3-3] エラー訂正処理

半導体メモリ219に保存された信号に対し、内符号P Iと外符号P Oを用いてエラー訂正回路209ではエラー箇所を検出し、エラー箇所のポインタフラグを立てる。

【0278】その後、半導体メモリ219から信号を読み出しながらエラーポインタフラグに合わせて逐次エラー箇所の信号を訂正し、内符号P Iと外符号P Oをはずしてデータ入出力インターフェース部30へ転送する。

【0279】ECCエンコーディング回路208から送られて来た信号をデータ入出力インターフェース部30から再生信号cとして出力する。

【0280】図10に上記情報記録再生装置1を用いたパーソナルコンピュータシステム構成を示す。

【0281】この場合、上記データ伝送インターフェース部8は情報記録再生装置1、情報再生装置122等に設けられるSCSI、ATAPI用のインターフェース回路に対応し、上記外部データ伝送インターフェース部7はSCSIボード138、IDEコントローラ120、IEEE1394.I/Fボード132に対応している。

【0282】[15] 一般的なパーソナルコンピュータシステム150の内部構造説明

【15-1】メインCPU111に直接接続されるデータ/アドレスライン

パーソナルコンピュータ150内のメインCPU111はメインメモリ112との間の情報入出力を直接行うメモリデータライン114と、メインメモリ112内に記録されている情報のアドレスを指定するメモリアドレスライン113を持ち、メインメモリ112内にロードされたプログラムに従ってメインCPU111の実行処理が進む。更にメインCPU111はI/Oデータライン146を通して各種コントローラとの情報転送を行うと共に、I/Oアドレスライン145のアドレス指定により情報転送先コントローラの指定と転送される情報内容の指定を行っている。

【0283】[15-2] CRTディスプレイコントロールとキーボードコントロール

CRTディスプレイ116の表示内容制御を行うLCD

コントローラ115はメモリデータライン114を介しメインCPU111間の情報交換を行っている。更に高解像度・豊富な表現色を実現するためCRTディスプレイ116専用のメモリとしてビデオRAM117を備えている。LCDコントローラ115はメモリデータライン114を経由してメインメモリ112から直接情報を入力し、CRTディスプレイ116に表示する事も出来る。

【0284】キーボード119から入力されたテンキー情報はキーボードコントローラ118で変換されてI/Oデータライン146を経由してメインCPU111に入力される。

【0285】[15-3] 内蔵型HDD/情報再生装置の制御系統

パーソナルコンピュータシステム150内に内蔵されたHDD121やCD-ROMドライブ・DVD-ROMドライブなどの光学式の情報再生装置122にはIDEインターフェースが使われることが多い。HDD121や情報再生装置122からの再生情報、またはHDD121への記録情報はIDEコントローラ120を経由してI/Oデータライン146に転送される。

【0286】特にブートディスクとしてHDD121を用いた場合にはパーソナルコンピュータシステム150起動時にメインCPU111がHDD121にアクセスし、必要な情報がメインメモリ112に転送される。

【0287】[15-4] 外部とのシリアル/パラレルインターフェース

パーソナルコンピュータシステム150の外部機器との情報転送にはシリアルラインとパラレルラインがそれぞれ用意されている。

【0288】“セントロ”に代表されるパラレルラインを制御するパラレルI/Fコントローラ123は例えばネットワークを介さずに直接プリンタ124やスキャナ125を駆動する場合に使われる。スキャナ125から転送される情報はパラレルI/Fコントローラ123を経由してI/Oデータライン146に転送される。またI/Oデータライン146上で転送される情報はパラレルI/Fコントローラ123を経由してプリンタ124へ転送される。

【0289】例えばCRTディスプレイ116に表示されているビデオRAM117内の情報やメインメモリ112内の特定情報をプリントアウトする場合、これらの情報をメインCPU111を介してI/Oデータライン146に転送した後、パラレルI/Fコントローラ123でプロトコル変換してプリンタ124に出力される。

【0290】外部に出力されるシリアル情報に関してはI/Oデータライン146で転送された情報がシリアルI/Fコントローラ130でプロトコル変換され、例えばRS-232C信号 ϕ として出力される。

【0291】[15-5] 機能拡張用バスライン

パーソナルコンピュータシステム150は機能拡張用に各種のバスラインを持っている。デスクトップのパーソナルコンピュータではバスラインとしてPCIバス133とEISAバス126を持っている場合が多い。各バスラインはPCIバスコントローラ143またはEISAバスコントローラ144を介してI/Oデータライン146とI/Oアドレスライン145に接続されている。バスラインに接続される各種ボードはEISAバス126専用ボードとPCIバス133専用ボードに分かれている。比較的PCIバス133の方が高速転送に向くため図9ではPCIバス133に接続しているボードの数が多くなっているが、それに限らずEISAバス126専用ボードを使用すれば例えばLANボード139やSCSIボード138をEISAバス126に接続する事も可能である。

【0292】[15-6] バスライン接続の各種ボードの概略機能説明

◎サウンドブラスターボード127：マイク128から入力された音声信号はサウンドブラスターボード127によりデジタル情報に変換され、EISAバス126、I/Oデータライン146を経由してメインメモリ112やHDD121、情報記録再生装置1に入力され、加工される。

【0293】また音楽や音声を聞きたい場合にはHDD121、141や情報再生装置122、情報記録再生装置1内に記録されているファイル名をユーザが指定する事によりデジタル音源信号がI/Oデータライン146、EISAバス126を経由してサウンドブラスターボード127に転送され、アナログ信号に変換された後、スピーカー129から出力される。

【0294】◎専用DSP137：有る特殊な処理を高速で実行したい場合、その処理専用のDSP137ボードをバスラインに接続する事が出来る。

【0295】◎SCSIインターフェース：外部記憶装置との間の情報入出力にはSCSIインターフェースを利用する場合が多い。情報バックアップ用MT（磁気テープ）142、外部据置き型HDD141、情報記録再生装置1等の外部記憶装置との間で入出力されるSCSIフォーマット情報をPCIバス133またはEISAバス126に転送するためのプロトコル変換や転送情報フォーマット変換をSCSIボード138内で実行している。

【0296】◎情報圧縮・伸長専用ボード：音声、静止画、動画像などマルチメディア情報は情報圧縮してHDD121、141や情報記録再生装置1（情報再生装置122）に記録される。

【0297】HDD121、141や情報記録再生装置1、情報再生装置122に記録されている情報を伸長してCRTディスプレイ116に表示したり、スピーカー129に鳴らす。またマイク128から入力された音声

信号などを情報圧縮してHDD121、141や情報記録再生装置1に記録する。

【0298】この情報の圧縮・伸長機能を各種専用ボードが受け持っている。音楽・音声信号の圧縮・伸長を音声符号化・復号化ボード136で行い、動画像（ビデオ映像）の圧縮・伸長をMPEGボード134で行い、サブピクチャー（副映像）の圧縮・伸長をサブピクチャーランレングス用ボード135で行っている。

【0299】【16】パーソナルコンピュータシステム150の外部ネットワークとの接続

【16-1】電話回線を用いたネットワーク接続
電話回線fを経由して外部に情報転送したい場合には、モデム131を用いる。すなわち希望の相手先へ電話接続するには図示して無いがNCU（Network Control Unit）が電話回線fを介して電話交換機に相手先電話番号を伝達する。電話回線が接続されると、シリアルI/Fコントローラ130がI/Oデータライン146上の情報に対して転送情報フォーマット変換とプロトコル変換を行い、その結果得られるデジタル信号のRS-232C信号をモデム131でアナログ信号に変換して電話回線fに転送される。

【0300】【16-2】IEEE1394を用いたネットワーク接続

音声、静止画、動画像などマルチメディア情報を外部装置（図示して無い）へ転送する場合にはIEEE1394インターフェースが適している。

【0301】動画や音声では一定時間内に必要な情報を送り切れないと画像の動きがギクシャクしたり、音声途切れたりする。その問題を解決するためIEEE1394では125 μ s毎にデータ転送が完了する isochronous 転送方式を採用している。IEEE1394ではこの isochronous 転送と通常の非同期転送の混在も許しているが、1サイクルの非同期転送時間は最大63:5 μ sと上限が決められている。この非同期転送時間が長過ぎると isochronous 転送を保証できなくなるためである。IEEE1394ではSCSIのコマンド（命令セット）をそのまま使用する事が出来る。

【0302】PCIバス133を伝わって来た情報に対し、isochronous 転送用の情報フォーマット変換やプロトコル変換、ノード設定のようなトポロジーの自動設定などの処理をIEEE1394I/Fボード132が行っている。

【0303】このようにパーソナルコンピュータシステム150内で持っている情報をIEEE1394信号gとして外部に転送するだけでなく、同様に外部から送られて来るIEEE1394信号gを変換してPCIバス133に転送する働きもIEEE1394I/Fボード132は持っている。

【0304】【16-3】LANを用いたネットワーク接続

企業内や官庁・学校など特定地域内のローカルエリア情報通信には図示して無いがLANケーブルを媒体としてLAN信号hの入出力を行っている。

【0305】LANを用いた通信のプロトコルとしてTCP/IP、NetBEUIなどが存在し、各種プロトコルに応じて独自のデータパケット構造（情報フォーマット構造）を持つ。PCIバス133上で転送される情報に対する情報フォーマット変換や各種プロトコルに応じた外部との通信手続き処理などをLANボード139が行う。

【0306】例としてHDD121内に記録して有る特定ファイル情報をLAN信号hに変換して外部のパーソナルコンピュータやEWS、あるいはネットワークサーバー（図示して無い）に転送する場合の手続きと情報転送経路について説明する。IDEコントローラ120の制御によりHDD121内に記録されているファイルディレクトリを出力させ、その結果のファイルリストをメインCPU111がメインメモリ112に記録すると共に、CRTディスプレイ116に表示させる。ユーザが転送したいファイル名をキーボード119入力するとその内容がキーボードコントローラ118を介してメインCPU111に認識される。メインCPU111がIDEコントローラ120に転送するファイル名を通知すると、HDDが内部の情報記録場所を判定してアクセスし、再生情報がIDEコントローラ120を経由してI/Oデータライン146に転送される。I/Oデータライン146からPCIバスコントローラ143にファイル情報が入力された後、PCIバス133を経由してLANボード139へ転送される。LANボード139では一連の通信手続きにより転送先とセッションを張った後、PCIバス133からファイル情報を入力し、伝送するプロトコルに従ったデータパケット構造に変換後LAN信号hとして外部へ転送する。

【0307】【17】情報再生装置または情報記録再生装置（光ディスク装置）からの情報転送

【17-1】標準的インターフェースと情報転送経路
CD-ROM、DVD-ROMなどの再生専用光ディスク装置である情報再生装置122やDVD-RAM、PD、MOなどの記録再生可能な光ディスクである情報記録再生装置1をパーソナルコンピュータシステム150内に組み込んで使用する場合、標準的なインターフェースとして“IDE”“SCSI”“IEEE1394”などが存在する。

【0308】一般的にはPCIバスコントローラ143やEISAバスコントローラ144は内部にDMAを持っている。DMAの制御によりメインCPU111を介在させる事無く各ブロック間で直接情報を転送する事が出来る。

【0309】例えば情報記録再生装置1の情報をMPEGボード134に転送する場合メインCPU111から

の処理はPCIバスコントローラ143へ転送命令を与えるだけで、情報転送管理はPCIバスコントローラ内のDMAに任せる。その結果、実際の情報転送時にはメインCPUは情報転送処理に悩殺される事無く並列して他の処理を実行できる。

【0310】同様に情報再生装置122内に記録されている情報をHDD141へ転送する場合もメインCPU111はPCIバスコントローラ143またはIDEコントローラ120へ転送命令を出すだけで、後の転送処理管理をPCIバスコントローラ143内のDMAまたはIDEコントローラ120内のDMAに任せている。

【0311】[17-2] 認証 (authentication) 機能

情報記録再生装置1もしくは情報再生装置122に関する情報転送処理には上述したようにPCIバスコントローラ143内のDMA、EISAバスコントローラ144内のDMAまたはIDEコントローラ120内のDMAが管理を行っているが、実際の転送処理自体は情報記録再生装置1もしくは情報再生装置122が持つ認証 (authentication) 機能部が実際の転送処理を実行している。

【0312】DVDビデオ、DVD-ROM、DVD-RなどのDVDシステムではビデオ、オーディオのビットストリームはMPEG2 Program streamフォーマットで記録されており、オーディオストリーム、ビデオストリーム、サブピクチャストリーム、プライベートストリームなどが混在して記録されている。情報記録再生装置1は情報の再生時にプログラムストリーム (Program stream) からオーディオストリーム、ビデオストリーム、サブピクチャストリーム、プライベートストリームなどを分離抽出し、メインCPU111を介在させる事無くPCIバス133を介して直接音声符号化復号化ボード136、MPEGボード134あるいはサブピクチャランレングス用ボード135に転送する。

【0313】同様に情報再生装置122もそこから再生されるプログラムストリーム (Program stream) を各種のストリーム情報に分離抽出し、個々のストリーム情報をI/Oデータライン146、PCIバス133を経由して直接 (メインCPU111を介在させる事無く) 音声符号化復号化ボード136、MPEGボード134あるいはサブピクチャランレングス用ボード135に転送する。

【0314】情報記録再生装置1や情報再生装置122と同様音声符号化復号化ボード136、MPEGボード134あるいはサブピクチャランレングス用ボード135自体にも内部に認証 (authentication) 機能を持っている。情報転送に先立ち、PCIバス133 (およびI/Oデータライン146) を介して情報記録再生装置1や情報再生装置122と音声符号化復号化ボード136、MPEGボード134、サブピクチャランレ

グス用ボード135間で互いに認証し合う。相互認証が完了すると情報記録再生装置1や情報再生装置122で再生されたビデオストリーム情報はMPEGボード134だけに情報転送する。同様にオーディオストリーム情報は音声符号化復号化ボード136のみに転送される。また静止画ストリームはサブピクチャランレングス用ボード135へ、プライベートストリームやテキスト情報はメインCPU111へ送られる。

【0315】次に、図1.0に示すMPEGボード134 (認証相手2) と情報記録再生装置1とのデータのやり取りについて、図1.1を用いて説明する。この場合、MPEGボード134と情報記録再生装置1との間に介在しているPCIバス133とSCSIボードについては説明を省略する。この場合、MPEGボード134にも認証機能部9を有し、認証情報記憶部24としては縦1列分の記憶がなされるようになっている。

【0316】すなわち、情報記録再生装置1からのAGID、設定エリア情報、ストリームIDからなるレポートキーコマンドがMPEGボード134に出力される(1)。

【0317】MPEGボード134は供給されたAGID、設定エリア情報、ストリームID (サブストリームID) に基づいてあらかじめ記憶されているストリームキーとエリアキーとを読み出し、この読み出したストリームキーとエリアキーとからなる合成キーで暗号化したチャレンジキーAを作成し、この暗号化されたチャレンジキーAを含むセンドキーコマンドを情報記録再生装置1に出力する(2)。

【0318】情報記録再生装置1は、供給されたチャレンジキーAに基づいて暗号化された暗号化キー1を生成し、この暗号化された暗号化キー1からなるレポートキーコマンドがMPEGボード134に出力される(3)。ついで、情報記録再生装置1は、あらかじめ記憶されているストリームキーとエリアキーとを読み出し、この読み出したストリームキーとエリアキーとからなる合成キーで暗号化したチャレンジキーBを生成し、チャレンジキーBを含むレポートキーコマンドがMPEGボード134に出力される(4)。

【0319】MPEGボード134は供給されたチャレンジキーBに基づいて暗号化された暗号化キー2を含むセンドキーコマンドを情報記録再生装置1に出力する(5)。

【0320】情報記録再生装置1は、供給された暗号化されている暗号化キー2から解読した暗号化キー2と上記作成した暗号化キー1とによりバスキーを作成する(6)。

【0321】また、MPEGボード134は供給された暗号化されている暗号化キー1から解読した暗号化キー1と上記作成した暗号化キー2とによりバスキーを作成する(6)。

【0322】上記例として(3)(4)の動作について詳細に説明する。

【0323】たとえば、相手から暗号化されたチャレンジキーが送られてきた時、つまりMPEGボード134から外部データ伝送インターフェース部7、データ伝送インターフェース部8を介して供給されるチャレンジキーを外部伝送データ記憶部25に記憶する。

【0324】ついで、暗号化部/復号化部/時変情報発生部23内のランダム信号発生器104の出力信号を暗号化キー1とし、シフトレジスタ109aからdの出力i5を入出力信号切り替え制御器106、バスライン26を介して認証情報記憶部24の自分が発行する暗号化キー1情報55に記憶させる。

【0325】これに続くランダム信号発生器104の一単位の数字を時変情報として、つまりシフトレジスタ109aからdの出力i5を入出力信号切り替え制御器106、バスライン26を介して認証情報記憶部24のランダム信号発生器104で作られるタイムリーな時変情報39に登録しておく。

【0326】チャレンジキーの解読まず、認証情報記憶部24の情報a対応のストリームキー情報31が読み出されてバスライン26、入出力信号切り替え制御器106を介してセクタ107に出力され、シフトレジスタ109aに送られる。

【0327】ストリームキー情報31が送り終り、第1エリアキー情報35が読み出されてバスライン26、入出力信号切り替え制御器106を介してセクタ107に出力され、シフトレジスタ109aに送られる。

【0328】この結果、シフトレジスタ109a、bにストリームキーが入り、シフトレジスタ109c、dに第1エリアキーが入る。

【0329】ここで合成キーの作成完了し、シフトレジスタ109aからdの出力i5として信号合成器105へ出力される。

【0330】次に、外部伝送データ記憶部25に記憶されていた暗号化されたチャレンジキーがバスライン26、入出力信号切り替え制御器106を介して入力i2として信号合成器105へ出力される。

【0331】信号合成器105は、供給される合成キーにより暗号化されたチャレンジキーが復号されたものがシフトレジスタ110d~aへ出力される。

【0332】外部伝送データ記憶部25からの56ビットのチャレンジキー送信終了後、シフトレジスタ110d~aに復号されたチャレンジキーがすべて入る。

【0333】この後、シフトレジスタ110d~aから出力されるチャレンジキーが入出力信号切り替え制御器106、バスライン26を介して認証情報記憶部24の相手が発行するチャレンジキー情報45に記憶される。

【0334】この相手が発行するチャレンジキー情報45を利用して自分が発行する暗号化キー1情報55を暗

号化する。

【0335】自分が発行するチャレンジキー情報51を認証情報記憶部24から読み出して、バスライン26、入出力信号切り替え制御器106を介してセクタ107に出力され、シフトレジスタ109aに送られる。

【0336】この結果、シフトレジスタ109aからdに自分が発行するチャレンジキー情報51が入る。このチャレンジキー情報51がシフトレジスタ109aからdの出力i5として信号合成器105へ出力される。

【0337】次に、自分が発行する暗号化キー1情報55を認証情報記憶部24から読み出して、バスライン26、入出力信号切り替え制御器106を介して入力i2として信号合成器105へ出力される。

【0338】信号合成器105は、供給される暗号化キー1情報55をチャレンジキー情報51により暗号化し、この暗号化された暗号化キー1がシフトレジスタ110d~aへ出力される。

【0339】この後、シフトレジスタ110d~aから出力される暗号化された暗号化キー1が入出力信号切り替え制御器106、バスライン26を介して外部伝送データ記憶部25に記憶される。

【0340】この外部伝送データ記憶部25に記憶された暗号化された暗号化キー1にレポートコマンド等を付与してデータ伝送インターフェース部8、外部データ伝送インターフェース部7を介してMPEGボード134へ送信される。

【0341】次に、認証情報記憶部24のランダム信号発生器104で作られるタイムリーな時変情報39が読み出されてバスライン26、入出力信号切り替え制御器106を介してセクタ107に出力され、シフトレジスタ109aからdに送られる。

【0342】すべての時変情報39が、シフトレジスタ109aからdに入ったらセクタ107を閉じる。これにより、ランダム信号発生器104の時変キーがランダム処理される。

【0343】バスキーの作成 暗号化キー1、暗号化キー2で作る。

【0344】すなわち、自分が発行する暗号化キー1情報55が認証情報記憶部24から読み出されて、バスライン26、入出力信号切り替え制御器106を介してセクタ107に出力され、シフトレジスタ109aに送られる。

【0345】この結果、シフトレジスタ109aからdに自分が発行する暗号化キー1情報55が入る。この暗号化キー1情報55がシフトレジスタ109aからdの出力i5として信号合成器105へ出力される。

【0346】また、相手が発行する暗号化キー2情報60が認証情報記憶部24から読み出されて、バスライン26、入出力信号切り替え制御器106を介して入力i2として信号合成器105へ出力される。

【0347】信号合成器105は、供給される暗号化キー1情報55と暗号化キー2情報60とが合成されてバスキーが生成され、シフトレジスタ109aからdの出力i5を入出力信号切り替え制御器106、バスライン26を介して認証情報記憶部24のバスキー情報65に記憶させる。

【0348】上記したように、メインCPU111が介在せずに、情報記録再生装置1と各処理ボード134、135、136とのデータの伝送を行えることができ、メインCPU111の負担を軽減でき、情報伝送期間中にメインCPU111が他の処理を行うことができる。

【0349】また、シフトレジスタ109a、からdを用いたランダム信号発生器104を用いることにより、非常に簡単な構成で暗号化／復号化（解読）を行える。

【0350】また、暗証機能部9内の時変情報発生部23で暗号鍵を発行するため、公開鍵を管理する第三者を置くことなく容易に相互認証可能、つまり第三者の介在や第三者への問い合わせ作業を不要とし、相互認証作業を非常に簡便にしかも信頼性高く行える。

【0351】また、暗証機能部9内で作成した暗号鍵を認証相手から送られた暗号鍵で暗号化して認証相手に伝送することにより、公開鍵方式を用いるよりも遙かに暗号化の信頼性が高く、情報漏洩を防げる。

【0352】また、情報記録媒体からの情報に付与されている情報の種類を示す情報（ストリームID）から認証相手を同定することにより、各認証相手に対して認証後、各認証相手にパラレルに情報を配信（送信）でき、この結果、各認証相手の負担が相対的に軽減すると共に情報記録媒体から情報再生を開始してから短時間で（TV）画面上に表示でき、タイムラグを最小に抑えることができる。

【0353】また、送信したい情報から認証相手を探ことができ、認証候補相手に対して情報を提供し、該当相手から回答してもらい、その回答結果に基づき相互認証作業に入るという方式により、比較的簡単な方法で認証相手を探すことができる。

【0354】また、認証機能部内に暗号化情報記憶用メモリを持たせることにより、メモリと独自のクロックを持つことにより情報を整理することができ、暗号化情報を認証機能部9独自のクロックで外部伝送データ記憶部25に事前に記録するため、データ伝送インターフェース部8は伝送回線の都合に応じて最適なタイミングで外部伝送データ記憶部25への情報の記録／再生処理を行うことができ、外部との間で送受信する暗号化情報を外部伝送データ記憶部25に一時保管し、更に内部に持つ独自のクロックに従って暗号化情報を独立して作成することにより、プロトコル変換時の適応性、外部通信回線混雑状況に対する柔軟性を向上させている。

【0355】また、エリアキー情報とストリームキー情報を認証情報記憶部24に事前に記憶しておき、その情

報を認証処理に利用することにより、認証局（CAセンタ）などの第三者の介在や第三者への問い合わせ作業を不要とし、相互認証作業を非常に簡便にしかも信頼性高く行える。

【0356】また、サーバから情報の配送・収集先のクライアント（のIPアドレスや電話番号）と配送・収集する情報内容を通知するだけで後の処理を情報記録再生装置1に任せるため、情報伝送中メインCPU111に負担をかけることがなく、情報伝送中もメインCPU111が他の処理をできるのでシステムとしての高速処理を可能とし、さらにコンピュータと情報再生装置間はネットワーク通信で情報の入出力を行うためコンピュータに対して情報再生装置を遠隔地に配置でき、この結果小さなスペースにコンピュータを配置することが可能となる。

【0357】また、情報再生装置が通信機能を持っているので、小型ノートPCなどのPCMCIAカードスロットが1個しかない小型PCでも通信用LANカードかモデムカードを利用すれば通信しながら情報再生装置間で情報の入出力処理が可能となる。さらに情報再生装置に認証機能を持ち暗号化情報を送れるので通信経路途中での情報コピー、情報漏洩の心配が無い。

【0358】さらに、通信機能部を有しただけでなく、認証機能部が通信機能部の通信機能を用いて認証相手との間で相互認証を行い、暗号化情報を伝送することにより、ネットワーク伝送経路途中での情報のコピーによる情報漏洩防止、セキュリティ確保が可能となる。

【0359】また、メモリに複数相手との認証履歴を記憶しておくことにより、時分割処理方法を利用して複数の認証相手に対して同時に認証処理と暗号化情報の伝送を可能とし、認証のため長時間待つ認証相手が無くなり、かつ高速で同時に複数の認証相手との認証処理を実行できる。

【0360】また、1個のランダム信号発生器104を用いて暗号鍵の発行と、情報の暗号化と、暗号化された情報の復号化（解読）の兼用処理を行え、信号合成器105を用いて暗号鍵の発行と、情報の暗号化と、暗号化された情報の復号化（解読）の兼用処理を行えるようにしたので、機能兼用化により回路の簡素化と低価格化が図れる。

【0361】また、パソコン内の各ボード間で認証処理を実施させることができる。

【0362】

【発明の効果】以上詳述したように、この発明によれば、メインの制御部が介在せずに、情報再生装置と各処理ボードとのデータの伝送を行えることができ、メインの制御部の負担を軽減でき、情報伝送期間中にメインの制御部が他の処理を行うことができる。

【0363】また、この発明によれば、非常に簡単な構成で暗号化／復号化（解読）を行える。

【0364】また、この発明によれば、公開鍵を管理する第三者を置くことなく容易に相互認証可能、つまり第三者の介在や第三者への問い合わせ作業を不要とし、相互認証作業を非常に簡便にしかも信頼性高く行える。

【0365】また、この発明によれば、伝送し合った暗号鍵で他方の暗号鍵を更に暗号化することにより、公開鍵方式を用いるよりも遙かに暗号化の信頼性が高く、情報漏洩を防げる。

【0366】また、この発明によれば、情報記録媒体からの情報に付与されている情報の種類を示す情報（ストリームID）から認証相手を同定することにより、各認証相手に対して認証後、各認証相手にパラレルに情報を配信（送信）でき、この結果、各認証相手の負担が相対的に軽減すると共に情報記録媒体から情報再生を開始してから短時間で（TV）画面上に表示でき、タイムラグを最小に抑えることができる。

【0367】また、この発明によれば、送信したい情報から認証相手を探すことができ、認証候補相手に対して情報を提供し、該当相手から回答してもらい、その回答結果に基づき相互認証作業に入るという方式により、比較的簡単な方法で認証相手を探すことができる。

【0368】また、この発明によれば、認証機能部内に暗号化情報記憶用メモリを持たせることにより、メモリと独自のクロックを持つことにより情報を整理することができ、暗号化情報を認証機能部独自のクロックで外部伝送データ記憶部に事前に記録するため、データ伝送インターフェース部は伝送回線の都合に応じて最適なタイミングで外部伝送データ記憶部への情報の記録／再生処理を行うことができ、外部との間で送受信する暗号化情報を外部伝送データ記憶部に一時保管し、更に内部に持つ独自のクロックに従って暗号化情報を独立して作成することにより、プロトコル変換時の適応性、外部通信回線混雑状況に対する柔軟性を向上させている。

【0369】また、この発明によれば、エリアキーとストリームキーを認証情報記憶部に事前に記憶しておき、その情報を認証処理に利用することにより、認証局（CAセンタ）などの第三者の介在や第三者への問い合わせ作業を不要とし、相互認証作業を非常に簡便にしかも信頼性高く行える。

【0370】また、この発明によれば、サーバから情報の配送・収集先のクライアント（のIPアドレスや電話番号）と配送・収集する情報内容を通知するだけで後の処理を情報再生装置に任せるため、情報伝送中メインCPUに負担をかけることがなく、情報伝送中もメインCPUが他の処理をできるのでシステムとして的高速処理を可能とし、さらにコンピュータと情報再生装置間はネットワーク通信で情報の入出力を行うためコンピュータに対して情報再生装置を遠隔地に配置でき、この結果小さなスペースにコンピュータを配置することが可能となる。

【0371】また、この発明によれば、情報再生装置が通信機能を持っているので、小型ノートPCなどのPCMCIAカードスロットが1個しかない小型PCでも通信用LANカードかモデムカードを利用すれば通信しながら情報再生装置間で情報の入出力処理が可能となる。さらに情報再生装置に認証機能を持ち暗号化情報を送れるので通信経路途中での情報コピー、情報漏洩の心配が無い。

【0372】さらに、通信機能部を有しただけでなく、認証機能部が通信機能部の通信機能を用いて認証相手との間で相互認証を行い、暗号化情報を伝送することにより、ネットワーク伝送経路途中での情報のコピーによる情報漏洩防止、セキュリティ確保が可能となる。

【0373】また、この発明によれば、メモリに複数相手との認証履歴を記憶しておくことにより、時分割処理方法を利用して複数の認証相手に対して同時に認証処理と暗号化情報の伝送を可能とし、認証のため長時間待つ認証相手が無くなり、かつ高速で同時に複数の認証相手との認証処理を実行できる。

【0374】また、この発明によれば、1個のランダム信号発生器を用いて暗号鍵の発行と、情報の暗号化と、暗号化された情報の復号化（解読）の兼用処理を行えるようにしたので、機能兼用化により回路の簡素化と低価格化が図れる。

【0375】また、この発明によれば、パソコン内の各ボード間で認証処理を実施させることができる。

【図面の簡単な説明】

【図1】図1は、この発明の実施の形態に係る認証機能を有する情報記録再生装置の構成を説明するブロック図である。

【図2】図2は、認証機能部の内部構造とそれに接続される周辺機器との関係を示す図である。

【図3】図3は、情報記録媒体に記録されているVOBUの内部構造説明図である。

【図4】図4は、パックの内部構成を示す図である。

【図5】図5は、認証作業手順を説明するためのフローチャートである。

【図6】図6は、認証情報記憶部に記憶される履歴情報内容を示す図である。

【図7】図7は、認証処理制御部の構成を説明するブロック図である。

【図8】図8は、暗号化部／復号化部／時変情報発生部の構成を説明するブロック図である。

【図9】図9は、情報記録再生装置内の情報記録再生部の構成を説明するブロック図である。

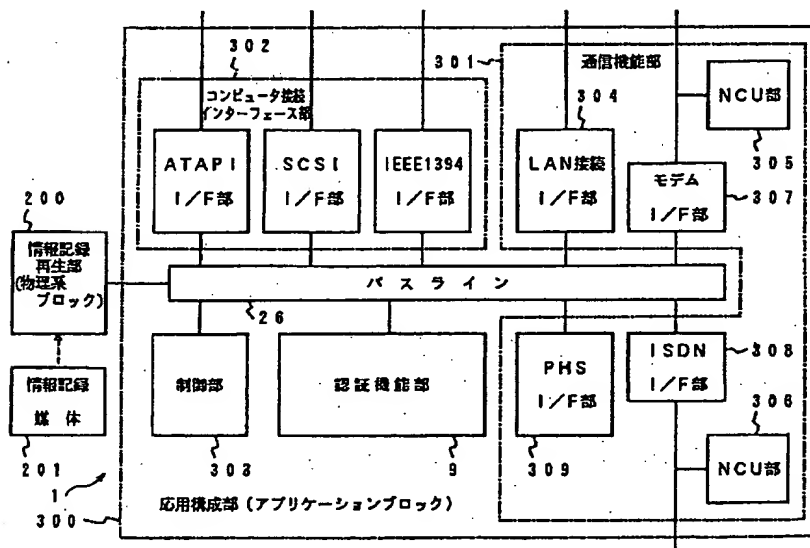
【図10】図10は、パーソナルコンピュータシステムの構成を説明するブロック図である。

【図11】図11は、MPEGボードと情報記録再生装置とのデータのやり取りを説明するための図である。

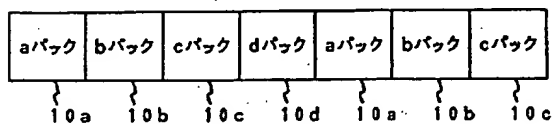
【符号の説明】

- 1…情報記録再生装置
 2～5…認証相手
 6、7…外部データ伝送インターフェース部
 8…データ伝送インタフェース部
 9…認証機能部
 10a…aパック
 10b…bパック
 10c…cパック
 10d…dパック
 11…パックヘッダ
 12…パケット
 13…パケットヘッダ
 14…伝達される情報内容
 21…基準クロック発生部
 22…認証処理制御部
 23…暗号化部／復号化部／時変情報発生部
 24…認証情報記憶部
 25…外部伝送データ記憶部
 26…バスライン
 30…データ入出力インターフェース部
 111…メインCPU
 120…IDEコントローラ
 122…情報再生装置
 127…サウンドブラスターボード
 130…シリアルI/Fコントローラ
 131…モデム
 132…IEEE1394 I/Fボード
 134…MPEGボード
 135…サブピクチャーランレングス用ボード
 136…音声符号化復号化ボード
 138…SCSIボード
 139…LANボード
 150…パーソナルコンピュータ
 200…情報記録再生部（物理ブロック）
 201…情報記録媒体

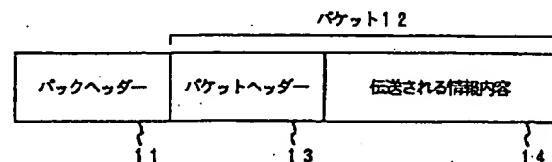
【図1】



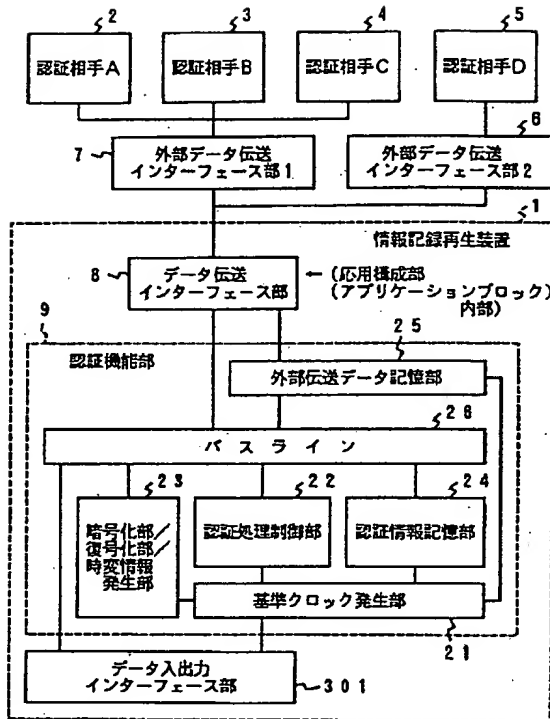
【図3】



【図4】



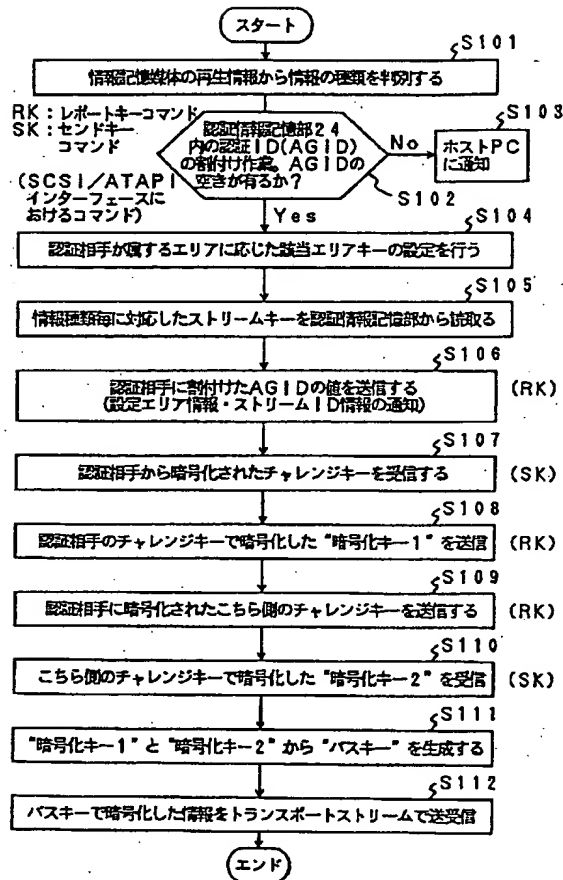
【図2】



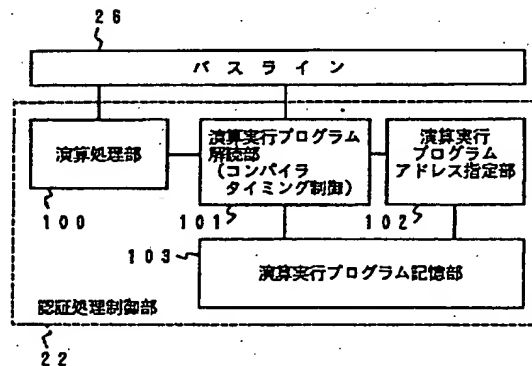
【図6】

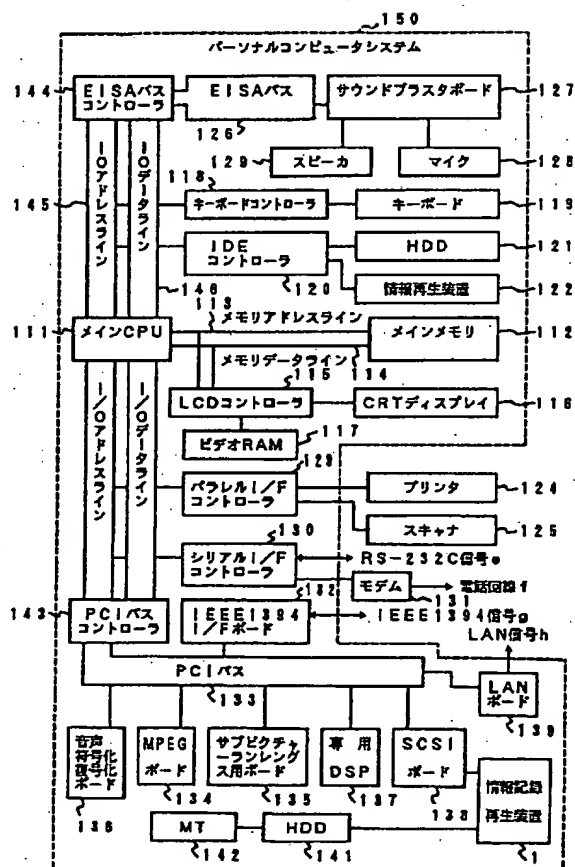
情報a対応の ストリームキー 情報 31	情報b対応の ストリームキー 情報 32	情報c対応の ストリームキー 情報 33	情報d対応の ストリームキー 情報 34
第1エリアキー 情報 35	第2エリアキー 情報 36	第3エリアキー 情報 37	第4エリアキー 情報 38
ランダム信号発生部で作られるタイムリーな時変情報 39			
AGID番号 (AGID=0) 40	AGID番号 (AGID=1) 41	AGID番号 (AGID=2) 42	AGID番号 (AGID=3) 43
相手が発行する チャレンジキー 情報(AGID=0) 45	相手が発行する チャレンジキー 情報(AGID=1) 46	相手が発行する チャレンジキー 情報(AGID=2) 47	相手が発行する チャレンジキー 情報(AGID=3) 48
自分が発行する チャレンジキー 情報(AGID=0) 51	自分が発行する チャレンジキー 情報(AGID=1) 52	自分が発行する チャレンジキー 情報(AGID=2) 53	自分が発行する チャレンジキー 情報(AGID=3) 54
自分が発行する 暗号化キー 1 情報(AGID=0) 55	自分が発行する 暗号化キー 1 情報(AGID=1) 56	自分が発行する 暗号化キー 1 情報(AGID=2) 57	自分が発行する 暗号化キー 1 情報(AGID=3) 58
相手が発行する 暗号化キー 2 情報(AGID=0) 60	相手が発行する 暗号化キー 2 情報(AGID=1) 61	相手が発行する 暗号化キー 2 情報(AGID=2) 62	相手が発行する 暗号化キー 2 情報(AGID=3) 63
バスキー情報 (AGID=0) 65	バスキー情報 (AGID=1) 66	バスキー情報 (AGID=2) 67	バスキー情報 (AGID=3) 68
AGID送信完了 情報(AGID=0) 70	AGID送信完了 情報(AGID=1) 71	AGID送信完了 情報(AGID=2) 72	AGID送信完了 情報(AGID=3) 73
チャレンジキー 受信完了情報 (AGID=0) 75	チャレンジキー 受信完了情報 (AGID=1) 76	チャレンジキー 受信完了情報 (AGID=2) 77	チャレンジキー 受信完了情報 (AGID=3) 78
暗号化キー 1 送信完了情報 (AGID=0) 80	暗号化キー 1 送信完了情報 (AGID=1) 81	暗号化キー 1 送信完了情報 (AGID=2) 82	暗号化キー 1 送信完了情報 (AGID=3) 83
チャレンジキー 送信完了情報 (AGID=0) 85	チャレンジキー 送信完了情報 (AGID=1) 86	チャレンジキー 送信完了情報 (AGID=2) 87	チャレンジキー 送信完了情報 (AGID=3) 88
暗号化キー 2 受信完了情報 (AGID=0) 90	暗号化キー 2 受信完了情報 (AGID=1) 91	暗号化キー 2 受信完了情報 (AGID=2) 92	暗号化キー 2 受信完了情報 (AGID=3) 93

【図5】

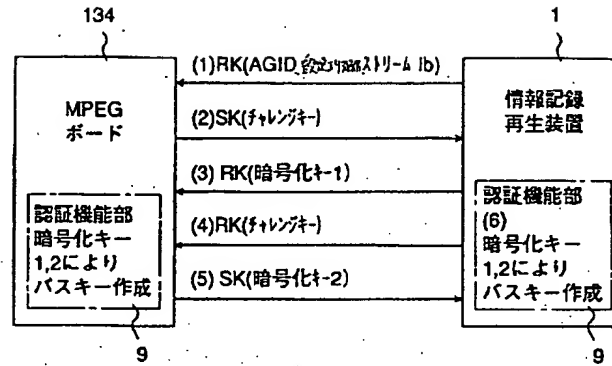


【図7】





【図11】



フロントページの続き

(51) Int. Cl. 6

識別記号

F I

H 0 4 L 9/00

6 7 5 A

(72) 発明者 石沢 良之

神奈川県川崎市幸区柳町70番地 株式会社
東芝柳町工場内